

New Features Guide

FortiManager 7.0.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 13, 2021

FortiManager 7.0.0 New Features Guide

02-700-698018-20210813

TABLE OF CONTENTS

Change Log	5
FortiManager 7.0 New Features Guide	6
Device Manager	7
Device and Groups	7
Model HA Cluster Wizard Improvements	7
More secure request authorization with OAuth protocol	9
Normalized interfaces support wildcard definition to match multiple objects 7.0.1	15
Centralized view for all detected devices within an ADOM 7.0.1	18
SD-WAN	19
New SD-WAN template	19
SD-WAN monitoring improvements	31
Templates	34
Interface template support for meta fields	35
Static route template with support for meta fields	40
Pre-defined IPsec template with recommended settings	45
Un-assign IPsec template to remove VPN-related configuration	47
CLI Template improvements 7.0.1	48
IPsec template enhanced support for tunnel interface configuration 7.0.1	51
Templates support assignment to device groups 7.0.1	53
Firmware Upgrades	55
Firmware template	56
Central Management	62
FortiSwitch Manager	62
FortiSwitch Manager central management improvements	62
FortiSwitch per-device management improvements	69
Diagnostics and tools for device health monitoring and registration with FortiCloud 7.0.1	73
Extender Manager	74
Extender Manager for central managed FortiExtender devices	74
FortiExtender Template for ZTP	78
Retrieve and display RSSI information for FGT-xx-3G4G models 7.0.1	79
Policy and Objects	82
Policy	82
Policy revision history	82
Assign multiple Global Policy Packages to the same ADOM, to different local Policy Packages 7.0.1	85
FortiGate 6000 and 7000 support for hit count 7.0.1	87
Objects	87
New IPS signatures monitoring page	88
Object revision history	92
System	96
High Availability (HA)	96
FortiManager verifies if FortiAnalyzer features are disabled before forming HA cluster	96
Cluster HA improvements 7.0.1	98

Administrators	99
Theme mode	99
Admin Permission to enable/disable script tab access	100
Admins can use a SAML SSO FortiCloud account to log in to FortiManager	102
ADOM	106
ADOM health check tool reports warnings on devices, configurations, and policy package status	106
Managing mixed FortiOS versions 6.2 and 6.4 in a single ADOM	109
Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM 7.0.1	112
ADOM upgrade from 6.4 to 7.0 7.0.1	114
Management Extensions	117
CPU and RAM maximum values for Management Extension Applications can be configured in CLI	117
New management extension - FortiSOAR	117
New management extension - FortiAIOps 7.0.1	120
New management extension - Universal Connector 7.0.1	123
Other	126
FortiManager Setup wizard	126
FortiManager VM licenses	131
Requesting and activating a trial license	131
Activating a new license	134
Activating an add-on license	136
GUI reorganization	138
Device Manager	139
AP Manager	140
FortiSwitch Manager	142
Extender Manager	144
VPN Manager	145
FortiManager VM supports Amazon EC2 IMDS version 2	146
Country list for direct registration 7.0.1	146
Event log easier to read 7.0.1	146
Local FortiGuard Distribution Server enhancements 7.0.1	147
FortiDeceptor and FortiTester	147
Download prioritization	148
IoT packages	150
NSX-T service template with VDOM support 7.0.1	151
Liveness detection	151
Service chain on FortiGate VMs	152
Manage devices using an NSX-T service template	153
CLI configuration	156

Change Log

Date	Change Description
2021-04-22	Initial release of FortiManager 7.0.0.
2021-04-27	Added New management extension - FortiSOAR on page 117.
2021-05-06	Added: <ul style="list-style-type: none">• Extender Manager for central managed FortiExtender devices on page 74• FortiExtender Template for ZTP on page 78
2021-05-17	Added <ul style="list-style-type: none">• More secure request authorization with OAuth protocol on page 9• Managing mixed FortiOS versions 6.2 and 6.4 in a single ADOM on page 109
2021-05-19	Added GUI reorganization on page 138.
2021-05-25	Added Firmware template on page 56.
2021-07-15	Initial release of FortiManager 7.0.1.
2021-07-26	Added New management extension - FortiAI Ops 7.0.1 on page 120.
2021-07-27	Added New management extension - Universal Connector 7.0.1 on page 123.
2021-08-09	Added: <ul style="list-style-type: none">• Diagnostics and tools for device health monitoring and registration with FortiCloud 7.0.1 on page 73.• CLI Template improvements 7.0.1 on page 48• IPsec template enhanced support for tunnel interface configuration 7.0.1 on page 51• FortiGate 6000 and 7000 support for hit count 7.0.1 on page 87• Assign multiple Global Policy Packages to the same ADOM, to different local Policy Packages 7.0.1 on page 85
2021-08-10	Added: <ul style="list-style-type: none">• Templates support assignment to device groups 7.0.1 on page 53• Cluster HA improvements 7.0.1 on page 98
2021-08-11	Added Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM 7.0.1 on page 112.
2021-08-12	Added ADOM upgrade from 6.4 to 7.0 7.0.1 on page 114.
2021-08-13	Added: <ul style="list-style-type: none">• Local FortiGuard Distribution Server enhancements 7.0.1 on page 147.• NSX-T service template with VDOM support 7.0.1 on page 151

FortiManager 7.0 New Features Guide

This document describes the new features added to FortiManager 7.0. The FortiManager new features are organized into the following categories:

- [Device Manager on page 7](#)
- [Central Management on page 62](#)
- [Policy and Objects on page 82](#)
- [System on page 96](#)
- [Management Extensions on page 117](#)
- [Other on page 126](#)

Device Manager

This section lists the new features added to FortiManager for the device manager:

- [Device and Groups on page 7](#)
- [SD-WAN on page 19](#)
- [Templates on page 34](#)
- [Firmware Upgrades on page 55](#)

Device and Groups

This section lists the new features added to FortiManager for devices and groups:

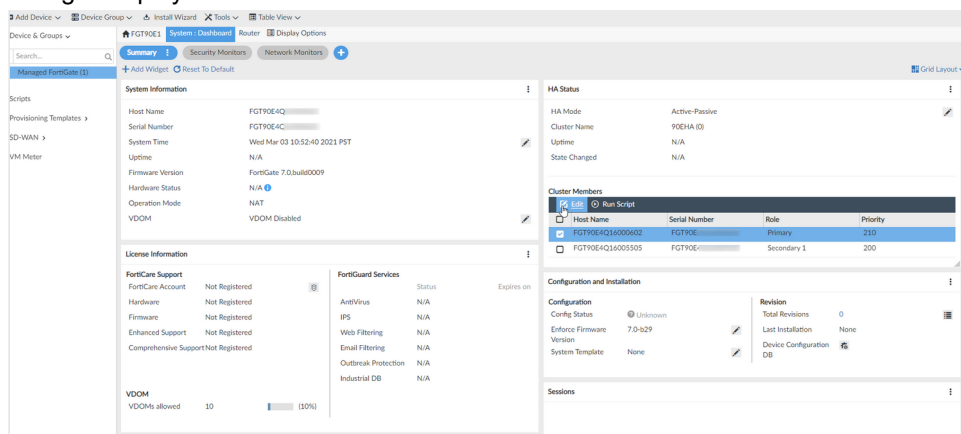
- [Model HA Cluster Wizard Improvements on page 7](#)
- [More secure request authorization with OAuth protocol on page 9](#)
- [Normalized interfaces support wildcard definition to match multiple objects 7.0.1 on page 15](#)
- [Centralized view for all detected devices within an ADOM 7.0.1 on page 18](#)

Model HA Cluster Wizard Improvements

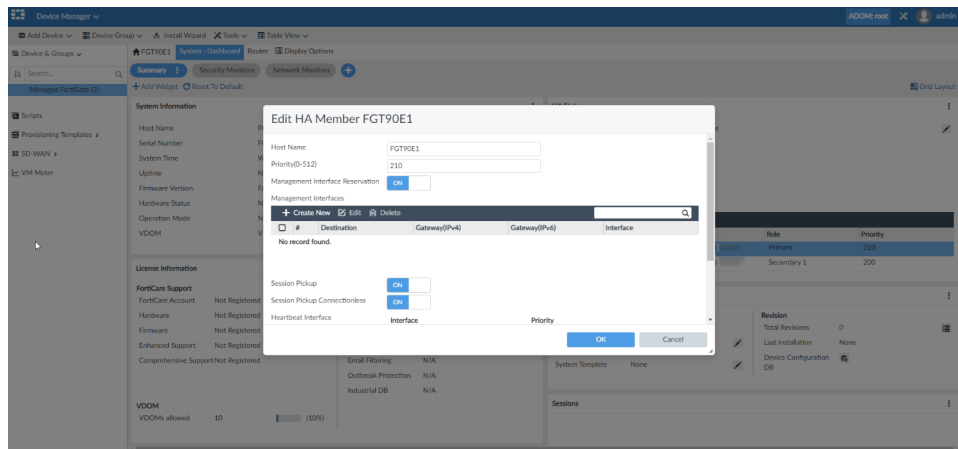
You can configure the member devices in an HA Cluster with the *HA Status* widget in the *Device Manager*.

To configure HA cluster member settings:

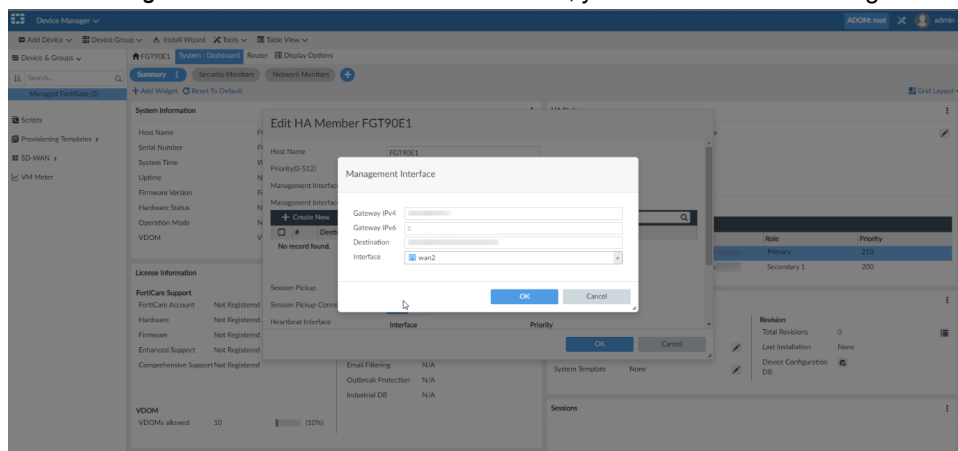
1. Go to *Device Manager > Device & Groups > Managed FortiGate*.
2. In *HA Status* widget, under *Cluster Members*, then select a member device, and click *Edit*. The *Edit HA Member* dialog is displayed.



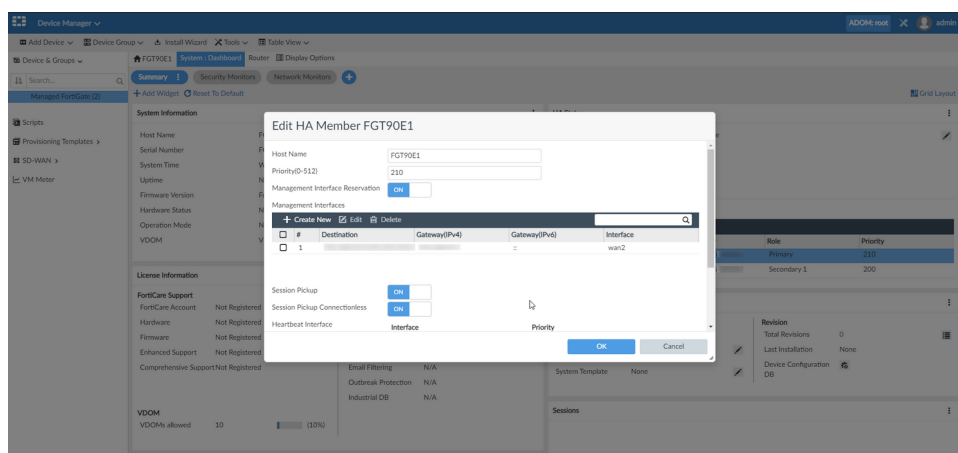
3. Configure the member *Host Name*, *Management Interface Reservation*, *Session Pickup*, and *Session Pickup Connectionless* settings.



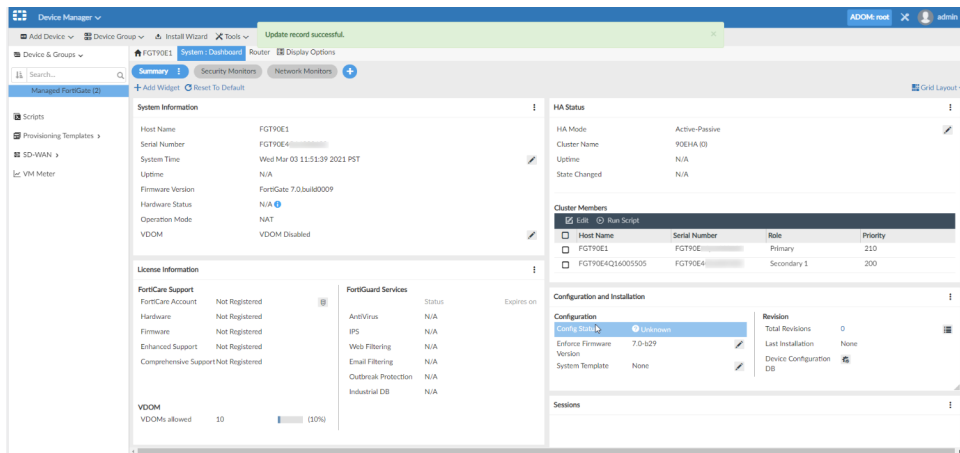
4. When *Management Interface Reservation* enabled, you can create new management interface.



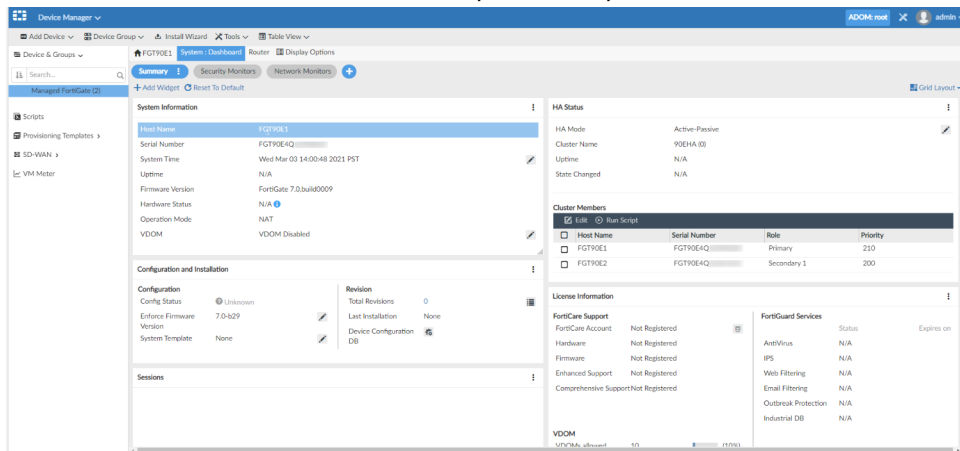
Click *Create New* to add a new interface.



Click *OK* to save the new interface.



5. Select another device in the cluster, and repeat the steps above.



More secure request authorization with OAuth protocol

FortiManager and FortiGate support the Open Authentication (OAuth) protocol to provide increased security for request authorization.

In FortiManager, the *Add Device* wizard supports the Open Authentication (OAuth) protocol to log in to FortiGate devices and authorize them for management by FortiManager. As an alternate to using the OAuth method, the *Add Device* wizard also supports the legacy device login method.

In FortiOS, the OAuth protocol is used when you create a fabric connector in FortiOS for FortiManager to request management by FortiManager.

This topic includes the following sections:

- [Using FortiManager Add Device wizard OAuth method on page 10](#)
- [Using FortiManager Add Device wizard legacy method on page 12](#)
- [Using FortiOS fabric connector for FortiManager on page 12](#)

Using FortiManager Add Device wizard OAuth method

The *Add Device* wizard in FortiManager now supports the OAuth protocol for device login and authentication.

When FortiGate is directly connected to FortiManager without NAT, the OAuth protocol can be used without setting an accessible IP address on FortiGate.

However when the OAuth protocol is used with the following network topologies, you must specify an accessible IP address on FortiGate for FortiManager to use:

- FortiGate is behind NAT with VIP.
- FortiManager and FortiGate are behind NAT and in the same network.

You can use the following CLI on the FortiGate to specify an accessible IP address for FortiManager to use:

```
config system global
  set management-ip <ip-address>
  set management-port <port>
end
```

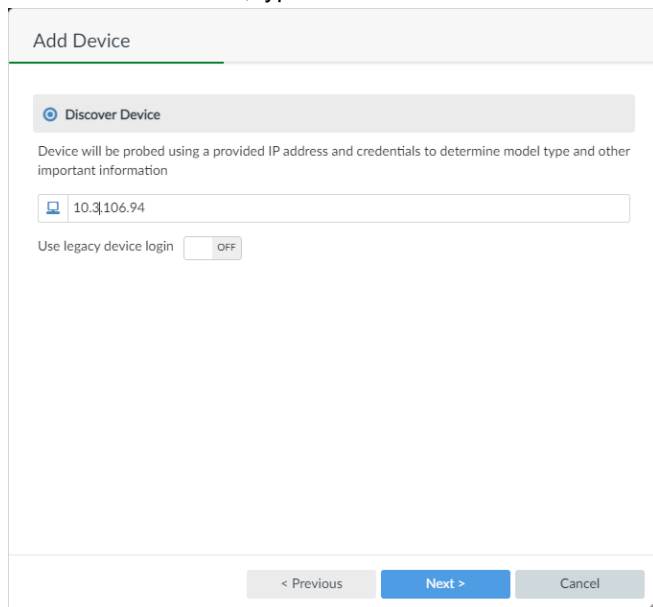
As an alternate to using the OAuth method, the *Add Device* wizard also supports the legacy device login method.

To use the new device login method with OAuth protocol:

1. In FortiOS, configure an accessible IP address on the FortiGate by using the following FortiOS command, if necessary:

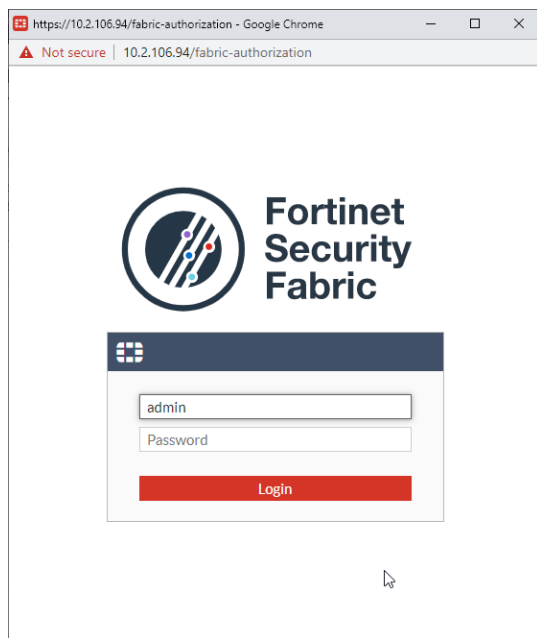
```
config system global
  set management-ip <ip-address>
  set management-port <port>
end
```

2. In FortiManager, go to *Device Manager*, and click *Add Device*. The *Add Device* wizard is displayed.
3. Click *Discover Device*.
4. In the *IP Address* box, type the IP address for the FortiGate, and click *Next*.

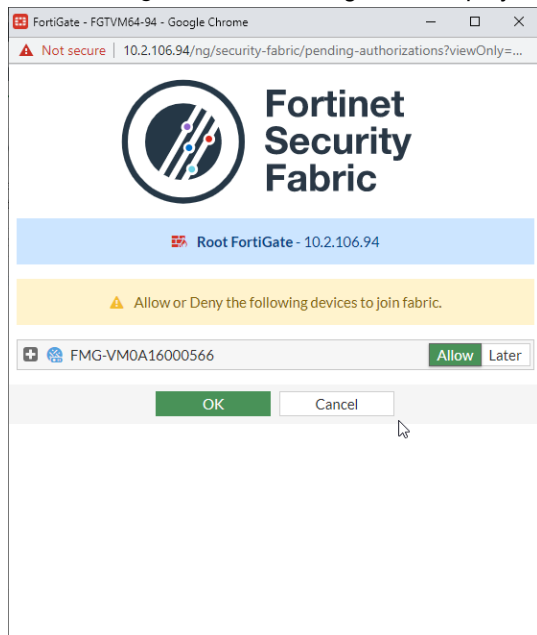


The screenshot shows the 'Add Device' wizard in FortiManager. The 'Discover Device' step is selected, indicated by a blue circle and the text 'Discover Device'. Below this, a message states: 'Device will be probed using a provided IP address and credentials to determine model type and other important information'. There is a text input field for the IP address, which currently contains '10.3.106.94'. Below the input field, there is a checkbox labeled 'Use legacy device login' which is currently set to 'OFF'. At the bottom of the wizard, there are three buttons: '< Previous' (disabled), 'Next >' (active), and 'Cancel' (disabled).

The *Fortinet Security Fabric* dialog box is displayed.



5. Complete the following options to log in to the device by using the OAuth method:
- In the *admin* box, type the username for the FortiGate device.
 - In the *Password* box, type the password for the FortiGate device.
 - Click *Login*. The next dialog box is displayed.



6. Click *Allow*, and click *OK* to authorize the device for management by FortiManager. The next dialog box in the wizard is displayed.
7. Complete the remaining screens in the wizard to finish adding the device.

Using FortiManager Add Device wizard legacy method

The *Add Device* wizard in FortiManager continues to support the legacy login method. The legacy login method does not use the OAuth protocol.

To use legacy device login:

1. Go to *Device Manager*, and click *Add Device*. The *Add Device* wizard is displayed.
2. Click *Discover Device*.
3. In the *IP Address* box, type the IP address for the FortiGate.
4. Toggle *Use legacy device login* to *ON*, and complete the following options to use legacy device login:
 - a. In the *User Name* box, type the username for the FortiGate device.
 - b. In the *Password* box, type the password for the FortiGate device.

The screenshot shows the 'Add Device' wizard in FortiManager, specifically the 'Discover Device' step. The wizard has a title bar 'Add Device' and a progress indicator. Below the title, there is a section titled 'Discover Device' with a sub-header 'Device will be probed using a provided IP address and credentials to determine model type and other important information'. There are three input fields: 'IP Address', 'User Name', and 'Password'. The 'Use legacy device login' toggle is set to 'ON'. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

5. Click *Next* to continue using the wizard and finish adding the device.

Using FortiOS fabric connector for FortiManager

From FortiOS, you can send a request to FortiManager for management by creating a fabric connector for FortiManager. In FortiOS, fabric connectors for FortiManager use the OAuth protocol for FortiManager authentication and authorization.

When FortiGate is directly connected to FortiManager or behind NAT with VIP, the OAuth protocol can be used without setting an accessible IP address on FortiManager.

When FortiManager and FortiGate are behind NAT and in the same network, you must specify an accessible IP address on FortiManager for FortiOS to use.

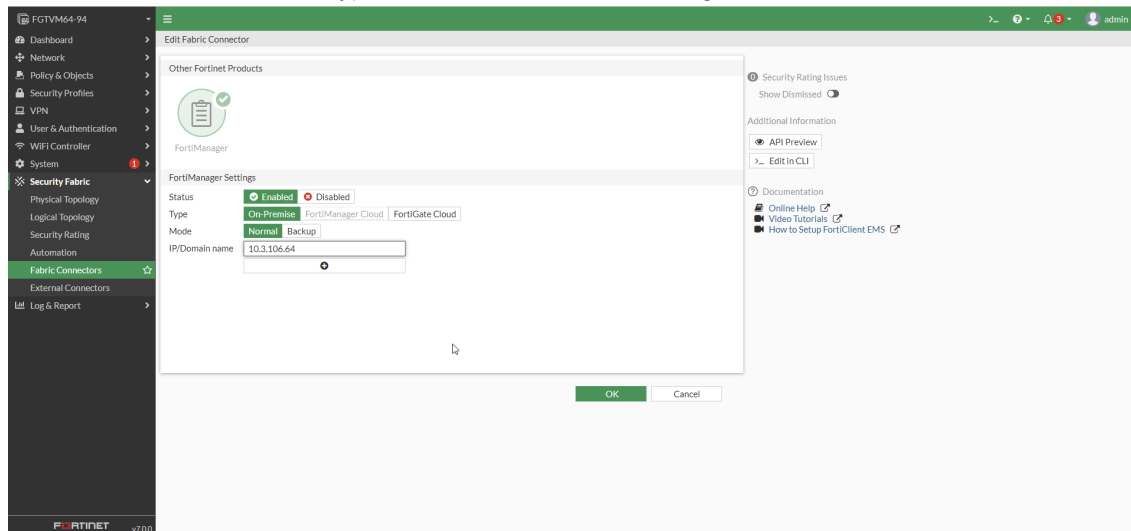
You can use the following CLI on FortiManager to specify an accessible IP address for FortiOS to use:

```
config system admin settings
  set auth-addr <ip-address>
  set auth-port <port>
end
```

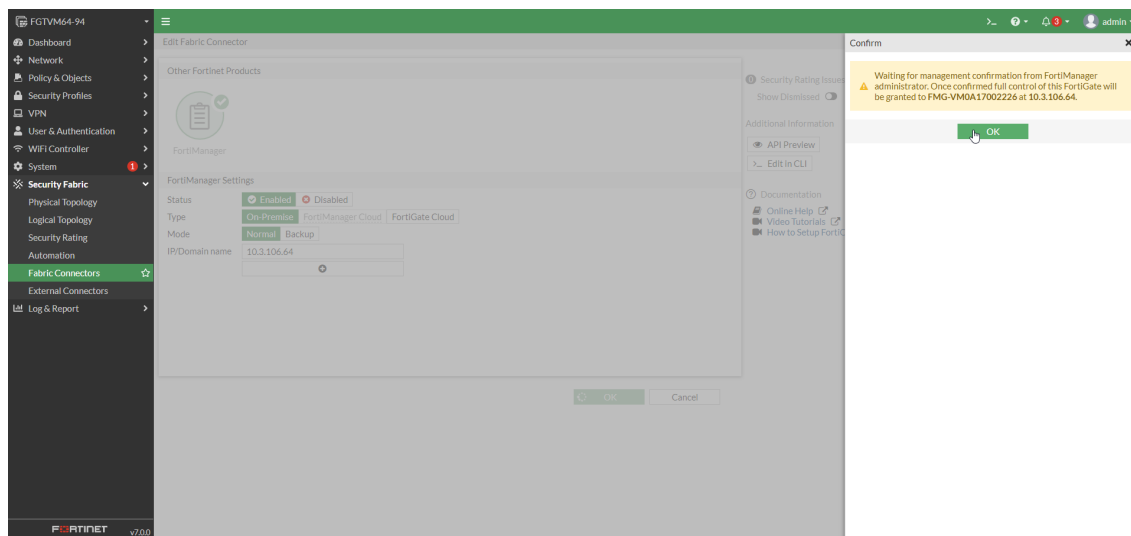

To use FortiGate fabric connectors:

1. In FortiManager, configure an accessible IP address by using the following FortiManager command, if necessary:

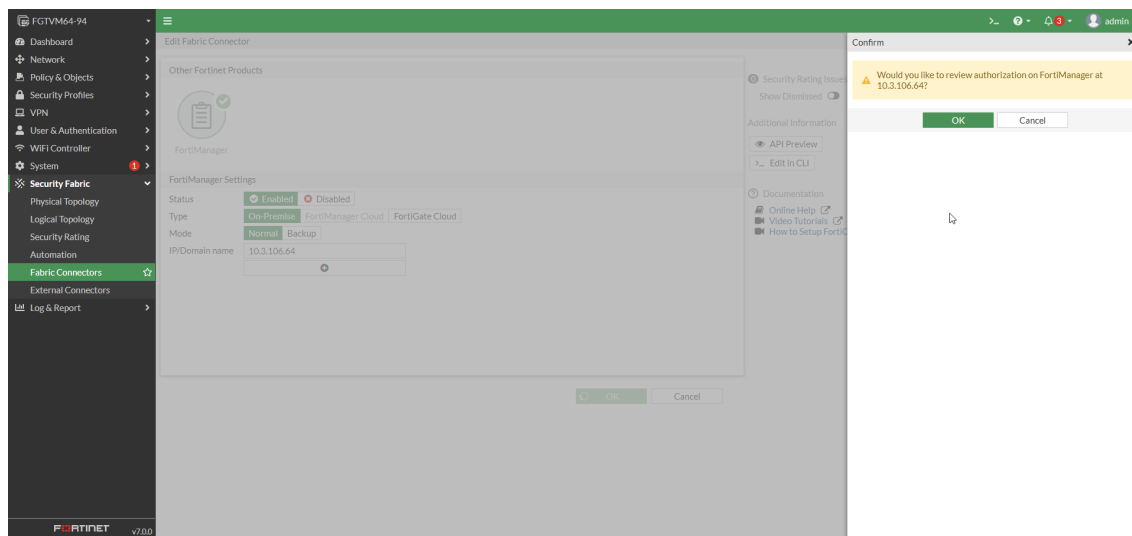
```
config system admin settings
  set auth-addr <ip-address>
  set auth-port <port>
end
```
2. In FortiOS, go to *Security Fabric > Fabric Connectors*, and double-click *FortiManager*. The *Edit Fabric Connector* pane is displayed.
3. In the *IP /Domain Name* box, type the IP address for FortiManager, and click *OK*.



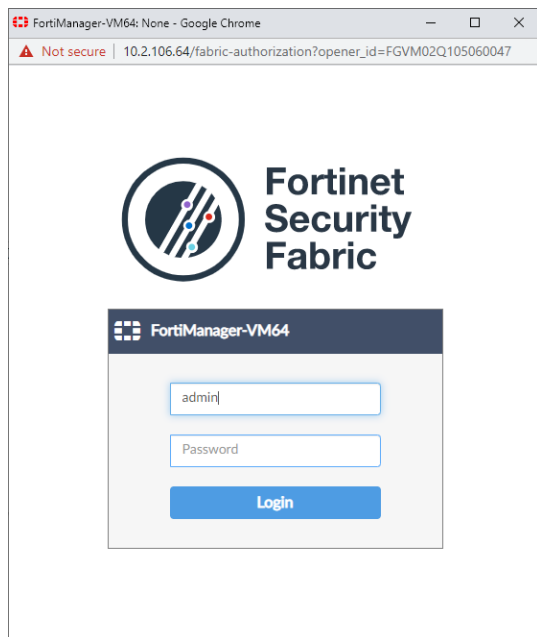
A *Confirm* pane is displayed and communicates that FortiOS sent the request to FortiManager.



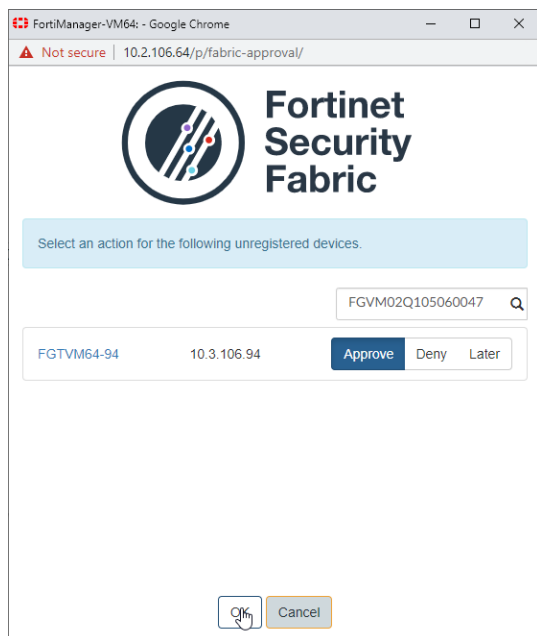
When communication with FortiManager is established, you can click *OK* to review authorization.



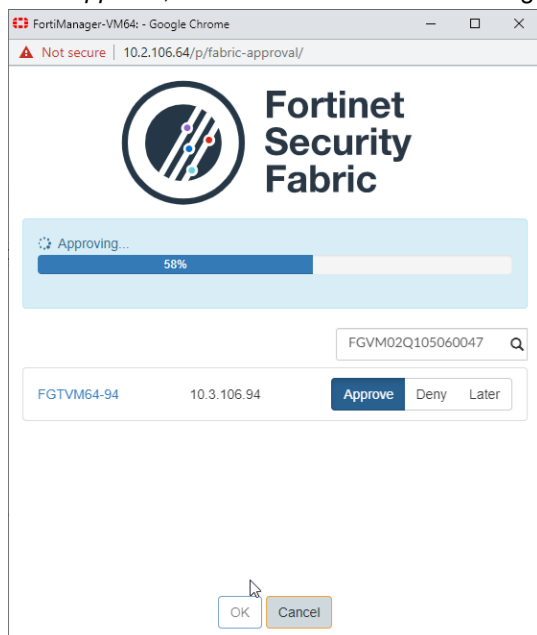
4. Click **OK** to review authorization.
The Fortinet Security Fabric dialog box is displayed.



5. Complete the following options to log in to the device by using the OAuth method:
 - a. In the *admin* box, type the username for the FortiManager device.
 - b. In the *Password* box, type the password for the FortiManager device.
 - c. Click *Login*. The next dialog box is displayed.



6. Click **Approve**, and click **OK** to authorize management by FortiManager. The request is approved and proceeds.



FortiGate is managed by FortiManager

Normalized interfaces support wildcard definition to match multiple objects - 7.0.1

Starting in FortiManager 7.0.1, normalized interfaces support wildcard definitions to match multiple objects.

To use the new wildcard definition in interfaces:

1. Create the wildcard interface.
 - The *Wildcard Interfaces* configuration is available when creating normalized interfaces.
 - This rule allows the use of "." as a wildcard character to match any single alphanumeric character, and "*" to represent zero or more characters.
 - Multiple interfaces can be mapped to this rule.
2. Use the wildcard interface in a policy.
 - The new wildcard interface is used in a Firewall Policy the same way a regular interface is, but is interpreted as one or more interface that matches the defined wildcard definition.
3. Install the policy.
 - During the install, all of the matched objects are installed on the FortiGate.

To create a wildcard interface:

1. Go to *Policy & Objects > Object Configurations > Normalized Interface*, and create a new normalized interface.
2. Set the *Wildcard* toggle to the *ON* position, and then enter a *Wildcard Interface* definition, for example "a".

Edit Normalized Interface

Name: a4

Description: [Empty]

Color: [Color Picker]

Wildcard: ☒ ON

Wildcard Interface: a...

(period sign) -- this represent a single alpha-numeric character, similar to regex = [a-zA-Z0-9]
(star sign) -- this represent zero or more characters regex = *

Revision

Change Note: [Empty]

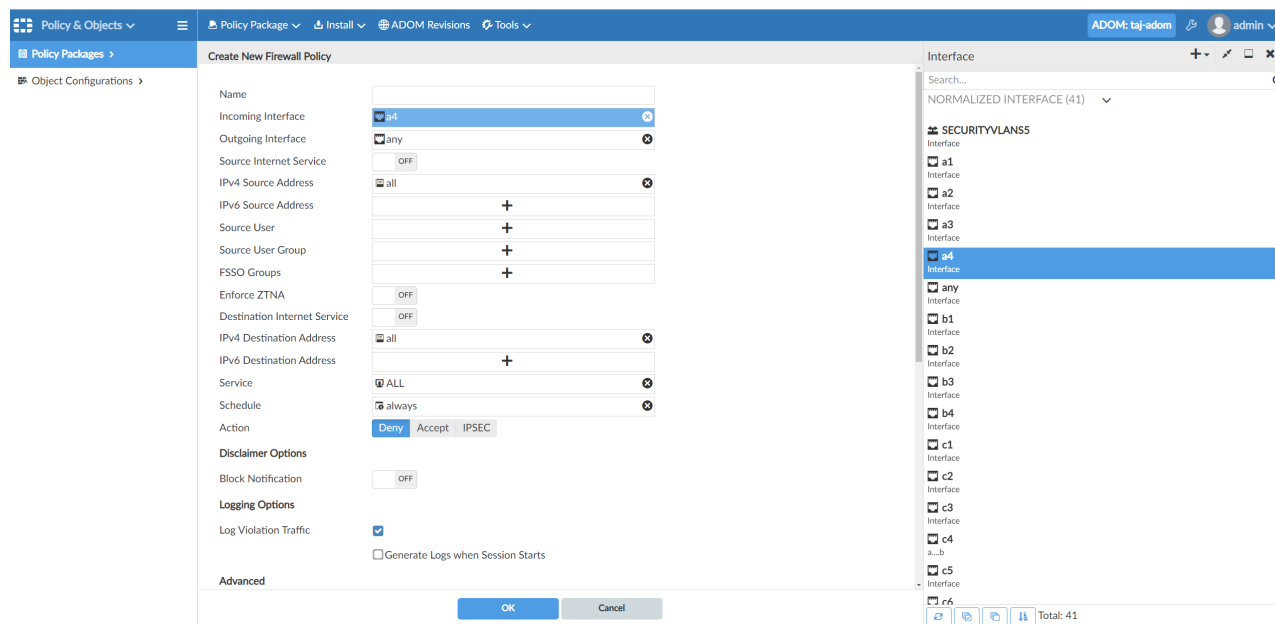
Revision History

Revert	View Diff	Column Settings					
	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note
<input type="checkbox"/>	2	admin	2021-06-01 15:54:42	a4	a4	Modify	1
<input type="checkbox"/>	1	admin	2021-06-01 15:50:54	a4	a4	Create	3

OK Cancel

Save the normalized interface.

3. Go to *Policy & Objects > Policy Packages*, and edit or create a Firewall Policy, and use the new wildcard interface in the policy.

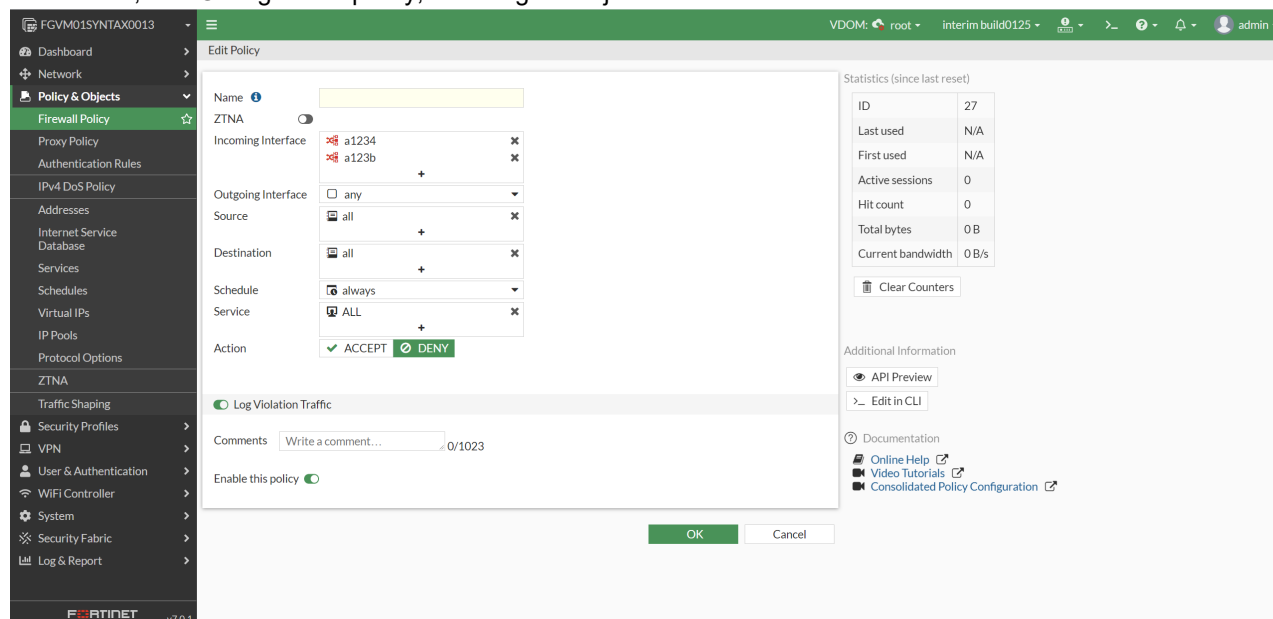


Save the Firewall Policy.

4. Install the Firewall Policy. During the install, all objects that match the wildcard definition are installed. In this example, the install preview shows that multiple objects matching the firewall definition will be installed.

```
config firewall policy
82: edit 27
83: set uuid d2c9c43c-c4ba-51ac-851c-a3e2657d0614
84: set srcintf "a1234" "a123b"
85: set dstintf "any"
86: set srcaddr "all"
87: set dstaddr "all"
88: set schedule "always"
89: set service "ALL"
90: set logtraffic all
91: next
92: end
```

5. After install, FortiGate gets the policy, including the objects that matched the wildcard definition.



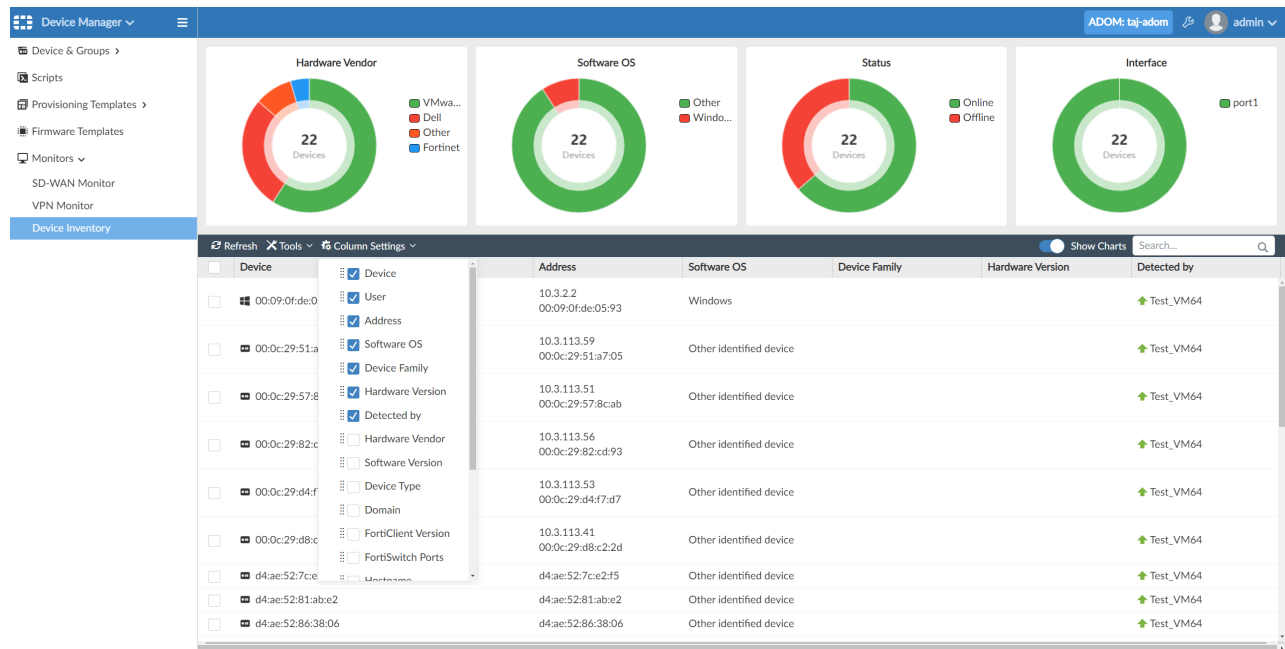
Centralized view for all detected devices within an ADOM - 7.0.1

Starting in FortiManager 7.0.1, a centralized view for detected devices within ADOM is available.

To use this feature, the FortiGate must enable *Device Detection* on the interface connecting to the network.

To view the centralized Device Inventory monitor:

1. Go to *Device Manager > Monitors > Device Inventory*.
The *Device Inventory* monitor displays a device inventory view for your current ADOM.



The *Device Inventory* monitor includes the following features.

- **Refresh:** Click *Refresh* to refresh the information displayed in the monitor.
- **Search:** Search for device inventory using the search field in the toolbar.
- **Filter:** Click *Column Settings* in the toolbar to change which columns are displayed in the table.
- **Export:** Click *Export* in the toolbar to export the *Device Inventory* information to a CSV.

SD-WAN

This section lists the new features added to FortiManager for SD-WAN:

- [New SD-WAN template on page 19](#)
- [SD-WAN monitoring improvements on page 31](#)

New SD-WAN template

With the new SD-WAN template, you can use Device VDOM meta fields in the member interface/ interface gateway, neighbor IP, and health-check server definitions.

In addition, how you enable and configure SD-WAN per-device management and central management has changed. You now use the following methods to enable and configure each:

- For per-device management, use the device database to configure SD-WAN settings on each device.
- For central management, use SD-WAN templates to configure SD-WAN settings on one or more devices. SD-WAN templates have moved in *Device Manager* to *Provisioning Templates*.

When you assign an SD-WAN template to a device, you have enabled SD-WAN central management for the device.

Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or

VPN interfaces.

When using SD-WAN templates with other types of provisioning templates, such as interface templates and IPsec templates, you should execute the templates in the following order:

- Interface template
- IPsec template
- SD-WAN template

This topic contains the following sections:

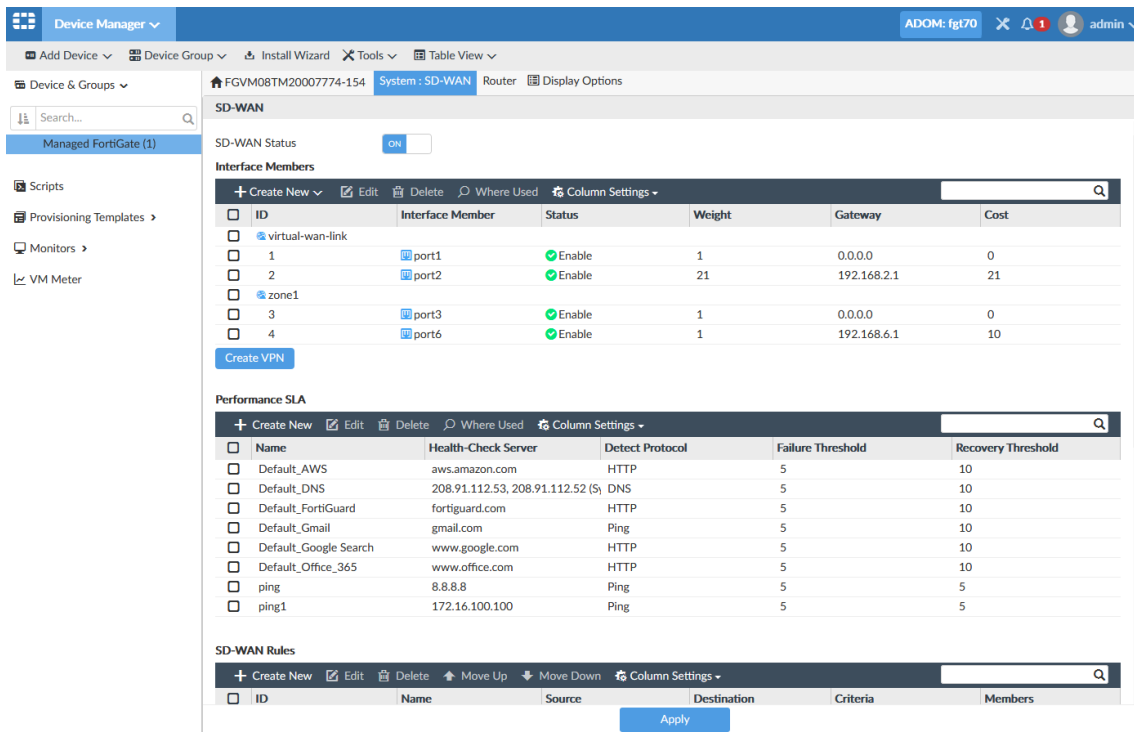
- [SD-WAN per-device management on page 20](#)
- [SD-WAN central management on page 21](#)
- [SD-WAN template support for meta fields on page 28](#)

SD-WAN per-device management

For SD-WAN per-device management, you can create, edit, and delete interface members, performance SLA, SD-WAN rules, Neighbor, and duplication. After configuring SD-WAN settings, install the configuration to the device.

To access SD-WAN per-device management:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Open the device database for the device:
 - a. Go to *Device Manager > Device & Groups*.
 - b. From the toolbar, select *Table View*.
 - c. In the tree menu, select a device group.
The devices in the group are displayed in the content pane.
 - d. In the content pane, double-click a device.
Alternately, select a device, and select *Configuration* from the *More* menu.
The device database is displayed in the content pane.
3. In the toolbar, click the *System* menu, and select *SD-WAN*.
The *SD-WAN* pane opens.



4. Configure the following sections for the device, and click *Apply*:

- Interface Members
- Performance SLA
- SD-WAN Rules
- Neighbor
- Duplication

5. Install the configuration to the device.

SD-WAN central management

For SD-WAN central management, you can create an SD-WAN template, and assign the template to one or more devices.

Normalized interfaces are not supported for SD-WAN templates. You can create multiple SD-WAN zones and add interface members to the SD-WAN zones. You must bind the interface members by name to physical interfaces or VPN interfaces.

Create performance SLA and SD-WAN rules. You can also configure BGP neighbors and packet duplication. Advanced configuration options are also available.

After configuring an SD-WAN template, assign the template to one or more devices, and then install the configuration to the devices.

To access SD-WAN central management:

1. If using ADOMs, ensure that you are in the correct ADOM.
2. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.
The SD-WAN templates are displayed.

3. Click *Create New*, and select *Template*.
The *SD-WAN Template* pane is displayed.

Edit SD-WAN Template

Name:

Description:

SD-WAN Status: ☒ ON

Interface Members

ID	Interface Member	Status	Weight	Gateway	Cost
1	port1	Enable	1	0.0.0.0	0
2	port2	Enable	21	192.168.2.1	21
3	port3	Enable	1	0.0.0.0	0
4	\$(int-mem)6	Enable	1	\$(int-mem-gw)	10

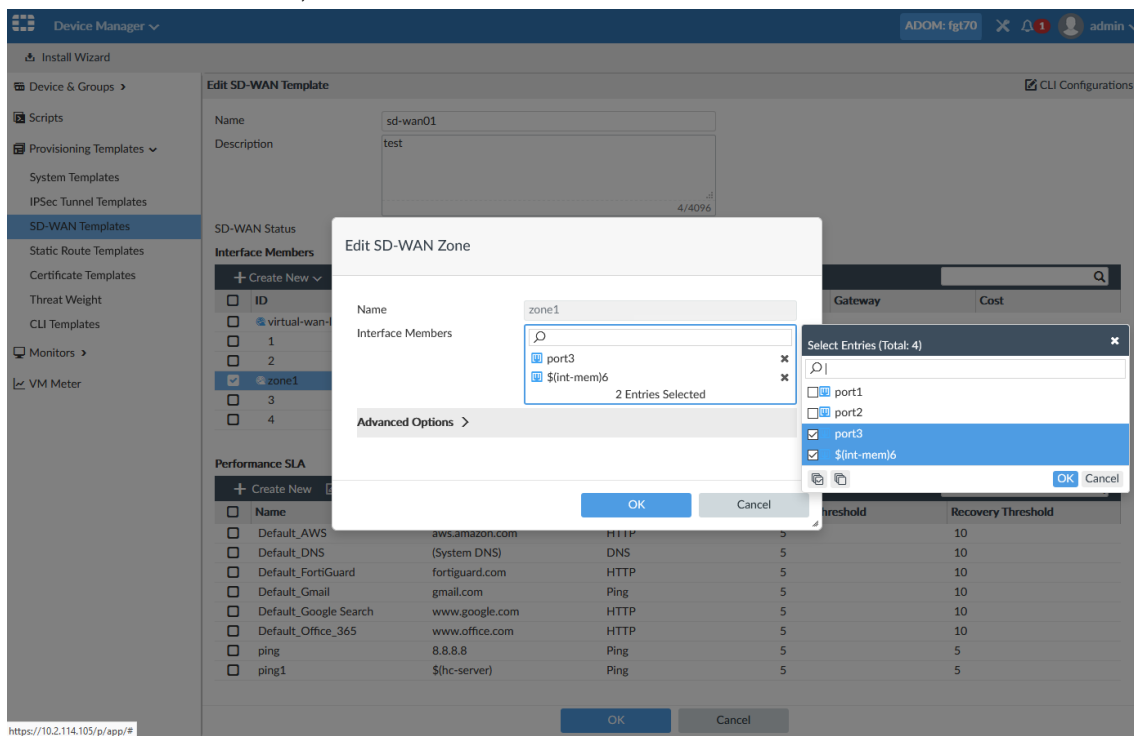
Performance SLA

Name	Health-Check Server	Detect Protocol	Failure Threshold	Recovery Threshold
Default_AWS	aws.amazon.com	HTTP	5	10
Default_DNS	(System DNS)	DNS	5	10
Default_FortiGuard	fortiguard.com	HTTP	5	10
Default_Gmail	gmail.com	Ping	5	10
Default_Google Search	www.google.com	HTTP	5	10
Default_Office_365	www.office.com	HTTP	5	10
ping	8.8.8.8	Ping	5	5
ping1	\$(hc-server)	Ping	5	5

OK Cancel

4. In the *Interface Members* section, create one or more zones:
 - a. Click *Create New* > *SD-WAN Zone*.
The *Create New SD-WAN Zone* dialog box is displayed.
 - b. In the *Name* box, type a name for the zone.

- c. Beside *Interface Members*, click the box to select interface members.



- d. Click OK.

The SD-WAN zone is created.

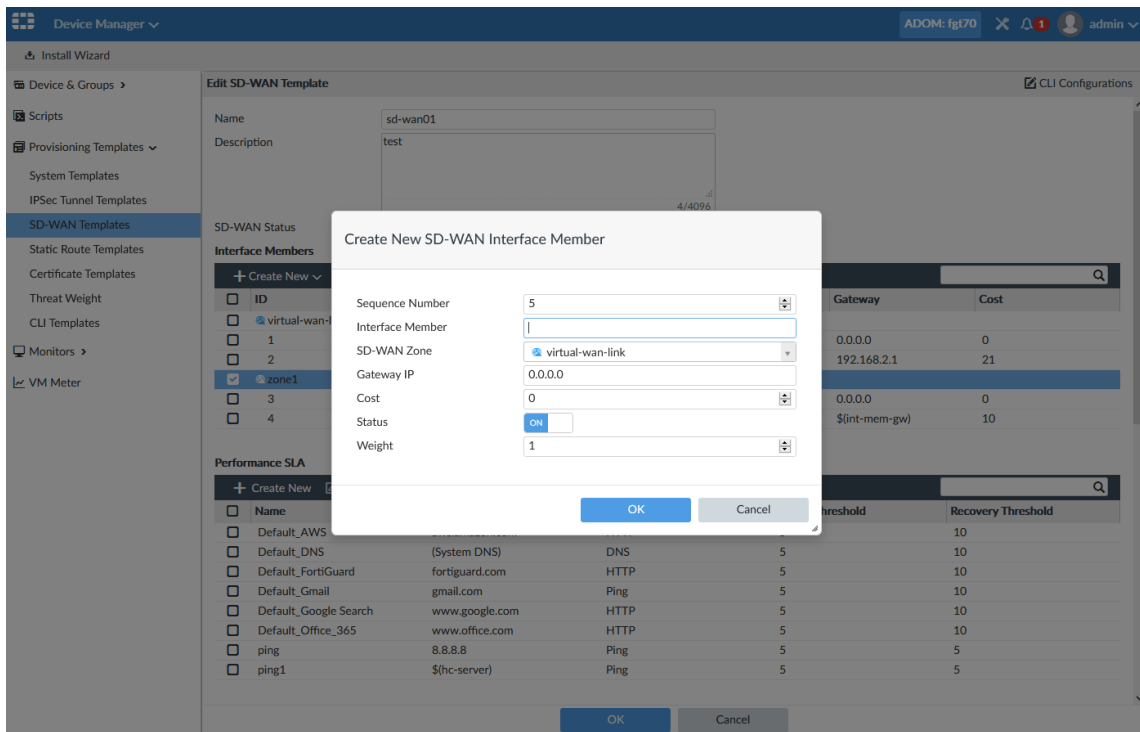
5. In the *Interface Members* section, create SD-WAN interface members:

- a. Click *Create New > SD-WAN Member*.

The *Create New SD-WAN Interface Member* dialog box is displayed.

- b. In the *Interface Members* box, type the name of the interface.

Bind the interfaces by name to physical or VPN interfaces.

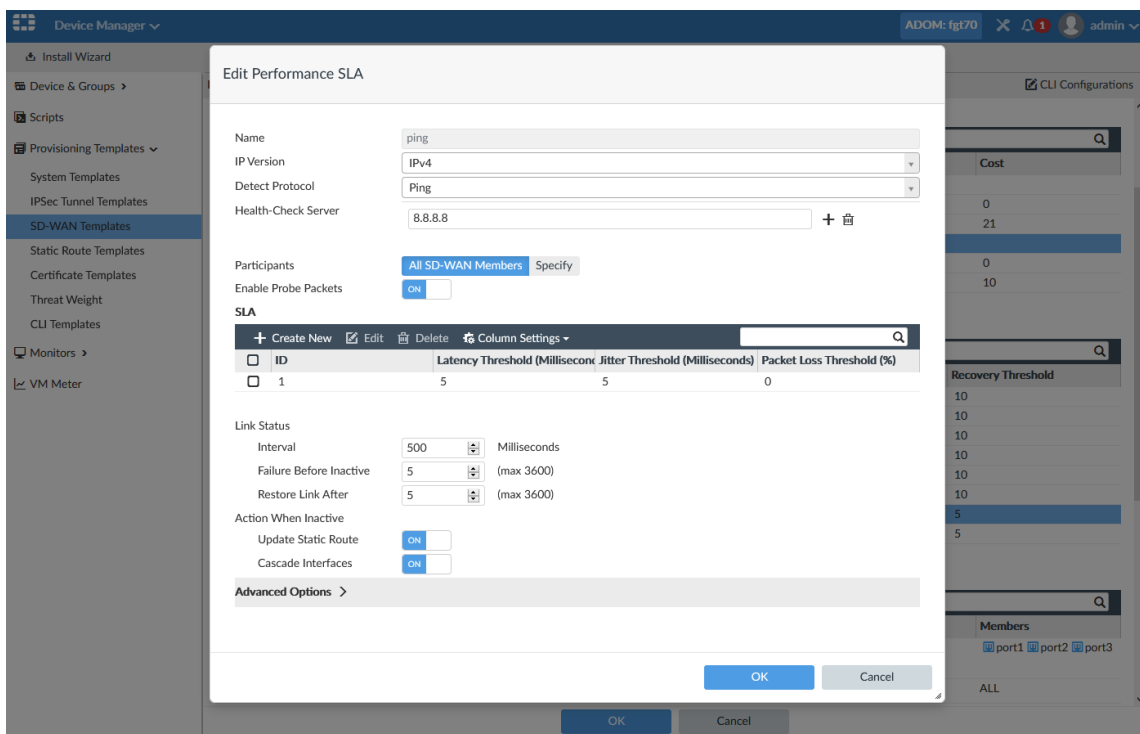


- c. Click OK.

The SD-WAN interface member is created.

6. Create Performance SLA:

- a. In the *Performance SLA* section, click *Create New*.
The *Performance SLA* dialog box is displayed.



- b. Complete the options, and click **OK**.
The Performance SLA settings are saved.

7. Create SD-WAN rules.

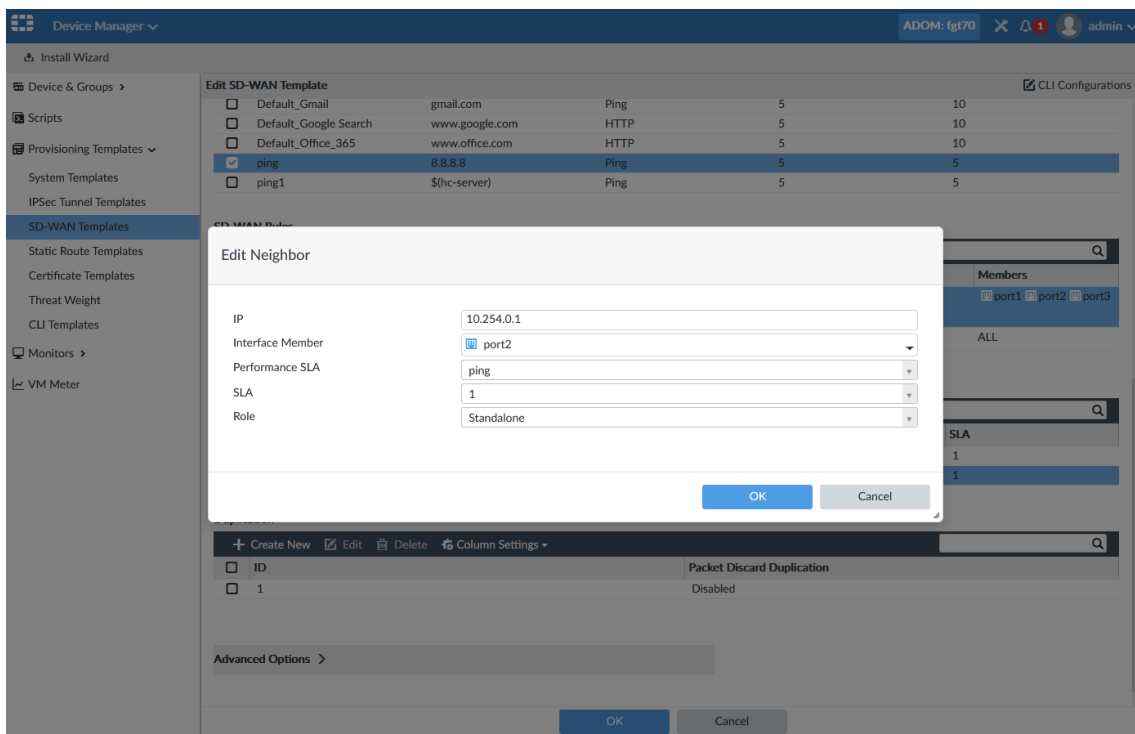
- a. In the *SD-WAN Rules* section, click *Create New*.
The *SD-WAN Rule* dialog box is displayed.

The screenshot shows the 'Edit SD-WAN Rule' dialog box in the FortiManager interface. The dialog is titled 'Edit SD-WAN Rule' and contains the following fields and options:

- Name:** rule01
- IP Version:** IPv4
- Source:**
 - Source Address:** Click here to select
 - Users:** Click here to select
 - User Groups:** Click here to select
- Destination:**
 - Address:** Internet Service
 - Internet Service:** A list of predefined services is shown, including 'Microsoft-Skype_Teams' and 'Snap-Snapchat'. Below the list, it says '2 Entries Selected'.
 - Internet Service Group:** Click here to select
 - Custom Internet Service:** Click here to select
 - Custom Internet Service Group:** Click here to select
 - Application:** Click here to select
 - Application Group:** Click here to select
- Type of Service:** 0x00
- Bit Mask:** 0x00
- Outgoing Interfaces:**
 - Strategy:** Manual, **Best Quality** (selected), Lowest Cost (SLA), Maximize Bandwidth (SLA)
 - Interface Preference:** A list of interfaces is shown, including 'port1', 'port2', and 'port3'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

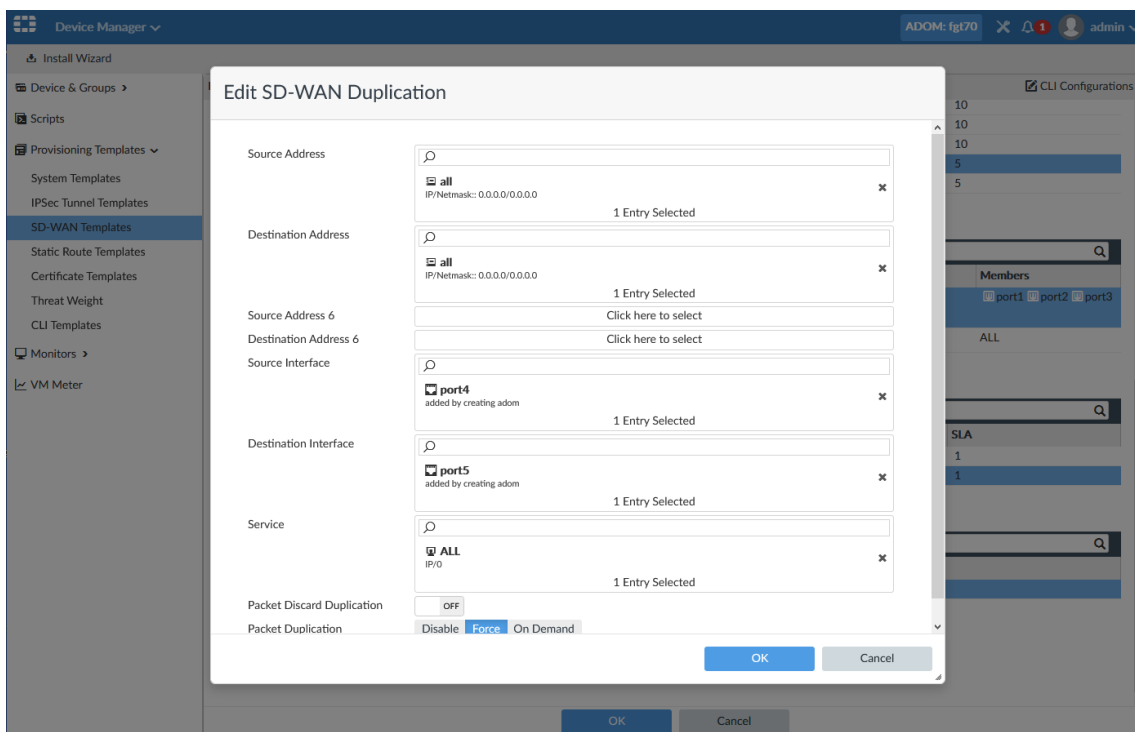
- b. Complete the options, and click **OK**.
The SD-WAN rules are saved.
8. Configure BGP neighbors.
- a. In the *Neighbor* section, click *Create New*.
The *Neighbor* dialog box is displayed.



- b. Complete the options, and click **OK**.
The neighbor settings are saved.

9. Configure packet duplication.

- a. In the *Duplication* section, click *Create New*.
The *Duplication* dialog box is displayed.



- b. Complete the options, and click **OK**.
The packet duplication settings are saved.

Edit SD-WAN Template

SD-WAN Rules

ID	Name	Source	Destination	Criteria	Members
1	rule01	ALL	Microsoft-Skype_Teams Snap-Snapchat	Latency (ping)	port1 port2 port3
	sd-wan	ALL	ALL	Volume	ALL

Neighbors

Neighbor	Role	Interface Member	Performance SLA	SLA
\$(nei-ip)	Standalone	port3	ping	1
10.254.0.1	Standalone	port2	ping	1

Duplication

ID	Packet Discard Duplication
1	Disabled

Advanced Options

duplication-max-num:

fail-detect:

neighbor-hold-boot-time:

neighbor-hold-down:

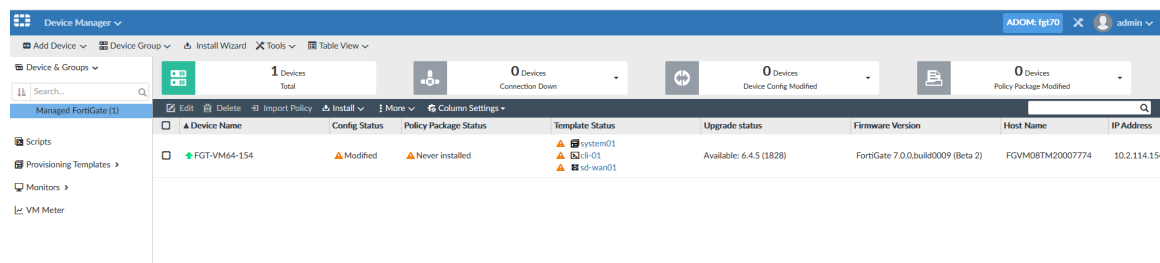
neighbor-hold-down-time:

OK **Cancel**

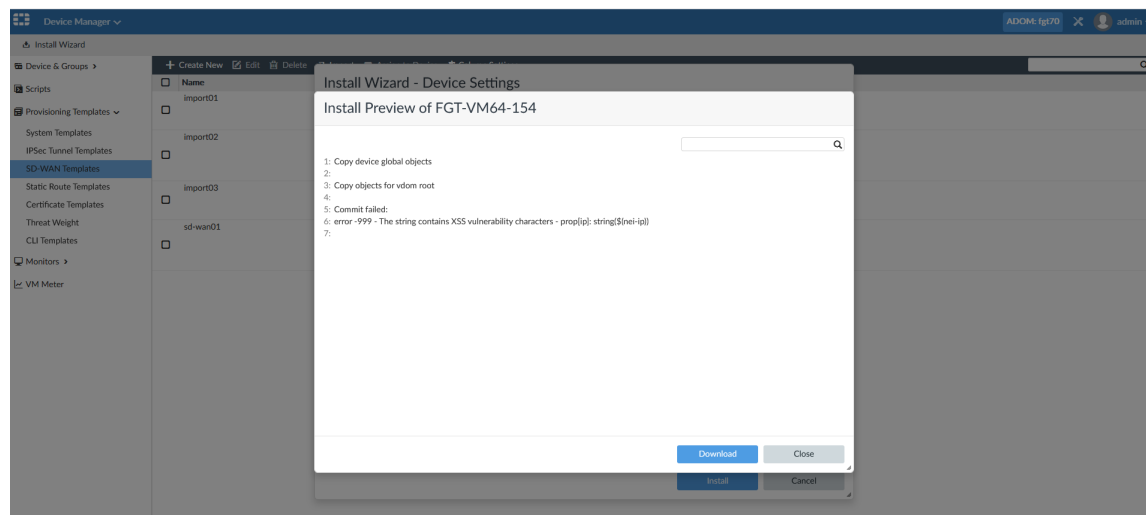
10. Click **OK**.
The SD-WAN template is saved.
11. Assign the SD-WAN template to one or more devices.
- Select the SD-WAN template, and click *Assign to Device*.
The *Assign to Device* dialog box is displayed.
 - In the *Available Entries* list, select the device, and click the right arrow to move the device to the *Selected Entries* list, and click **OK**.
The SD-WAN template is assigned to the device.

Name	Assigned to Devices	Interfaces	Description
import01		port1 port2 port3	
import02		port1 port2 port3 port6	
import03		port1 port2 port3	
sd-wan01	FGT-VM64-154 [root]	port1 port2 port3 \$(int-mem)6	test

12. Go to *Device Manager > Device & Groups*, and view the assigned provisioning templates in the *Template Status* column.



13. Click *Install Wizard* to install the device settings.
You can preview the settings.



SD-WAN template support for meta fields

SD-WAN templates support Device VDOM meta fields. You can use meta fields in SD-WAN templates for the following options:

- SD-WAN interface member
 - Interface member option
 - Gateway IP option
- Neighbor
 - IP option
- Performance SLA
 - Health-Check Server option

To create meta fields:

1. Go to *System Settings > Advanced > Meta Fields*.
2. Click *Create New*.
The *Create New Meta Fields* pane is displayed.

3. In the *Object* box, select *Device VDOM*.

4. In the *Name* box, type a name for the meta field.

The name of the field becomes the variable name that you can use in SD-WAN templates.

5. In the *Values* area, click *Create New* to define a value for one or more devices.

6. Click *OK*.

The meta field is created.

System Settings

Dashboard

All ADOMs

Network

HA

Admin

Administrators

Profile

Workspace

Remote Authentication Server

Admin Settings

SAML SSO

Certificates

Local Certificates

CA Certificates

CRL

Remote Certificates

Event Log

Task Monitor

Advanced

SNMP

Mail Server

Syslog Server

Meta Fields

Advanced Settings

Create New

Edit

Delete

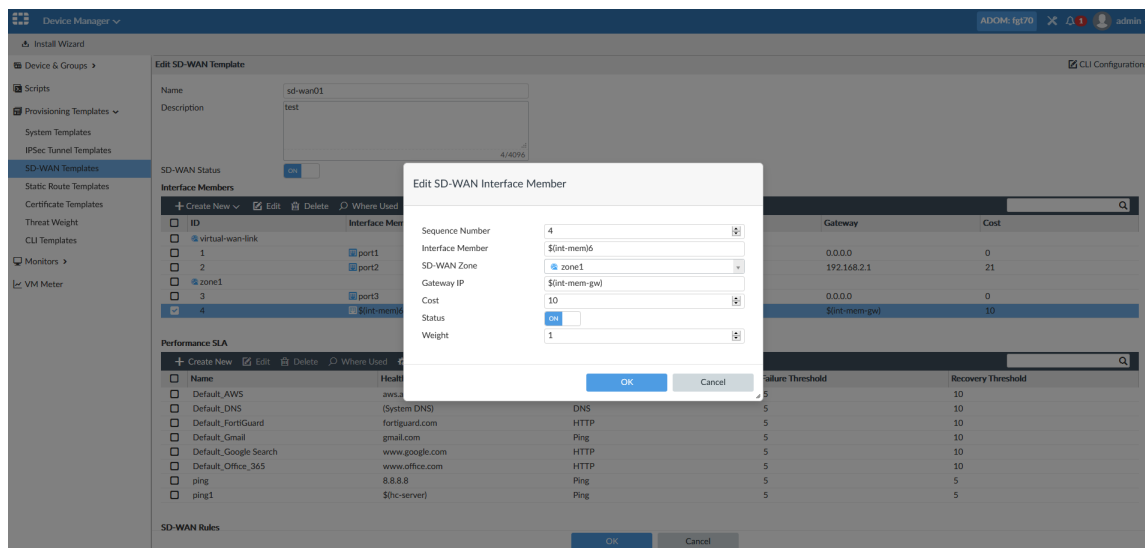
Collapse All

Expand All

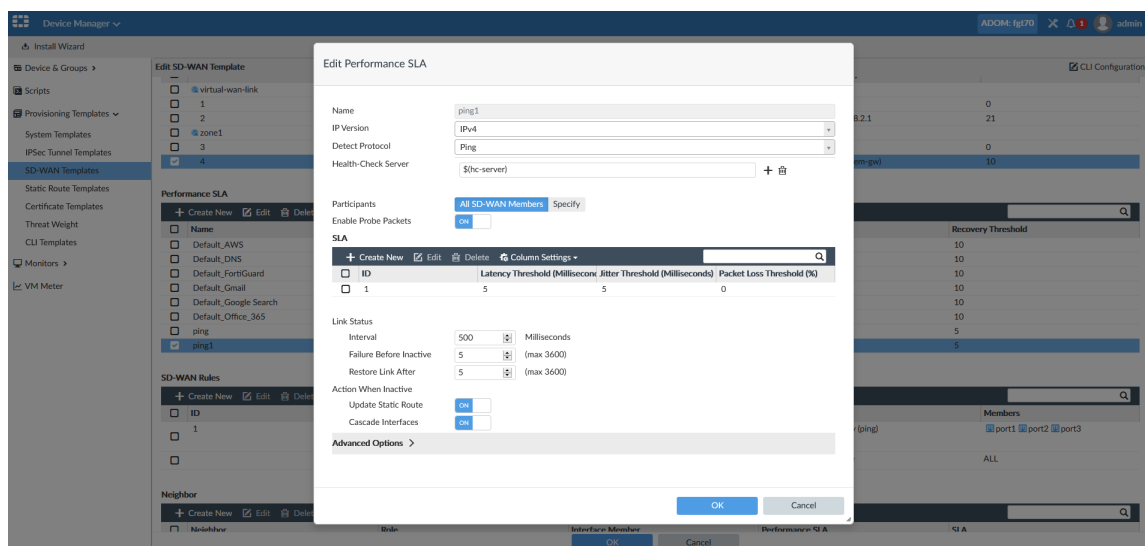
Column Settings

Meta Fields	Length	Importance	Status
System Administrator (2)			
Contact Email	50	Optional	Enabled
Contact Phone	50	Optional	Enabled
Device (6)			
Company/Organization	50	Optional	Enabled
Contact Email	50	Optional	Enabled
Contact Phone Number	50	Optional	Enabled
Address	150	Optional	Enabled
Interface	20	Required	Enabled
Ip-mask	20	Required	Enabled
Device Group (3)			
Device VDOM (4)			
hc-server	20	Required	Enabled
int-mem	20	Required	Enabled
int-mem-gw	20	Required	Enabled
net-ip	20	Required	Enabled
Administrative Domain (3)			
Firewall Address (3)			
Firewall Address Group (3)			
Central NAT (3)			
Firewall Service (3)			
Firewall Service Group (3)			
Firewall Policy (3)			

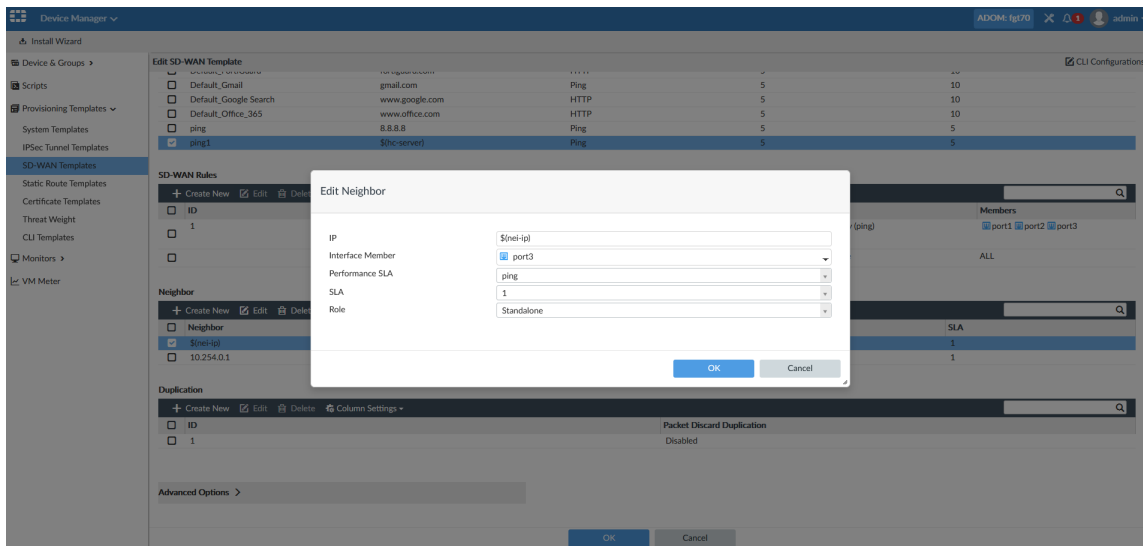
In the following SD-WAN template example, meta fields are used for the following interface member options: *Interface Member* and *Gateway IP*:



In the following SD-WAN template example, a meta field is used for the *Health-Check Server* option in Performance SLA:



In the following SD-WAN template example, a meta field is used for the *IP* option in Neighbor:



SD-WAN monitoring improvements

SD-WAN Monitor now includes information about ADVPN shortcut interfaces for monitoring SD-WAN networks. When device history monitoring is enabled for *SD-WAN Monitor*, the device history also includes information about ADVPN shortcut interfaces.

Monitoring SD-WAN interfaces (without shortcuts)

When an SD-WAN network is configured without ADVPN shortcuts, no shortcut information is displayed on *VPN Monitor* and on the graphs on *SD-WAN Monitor*.

In this example, device history monitoring is disabled for *SD-WAN Monitor*.

To view VPN monitor:

1. Go to *Device Manager > Monitors > VPN Monitor*.
The *VPN Monitor* is displayed. No shortcuts are configured.

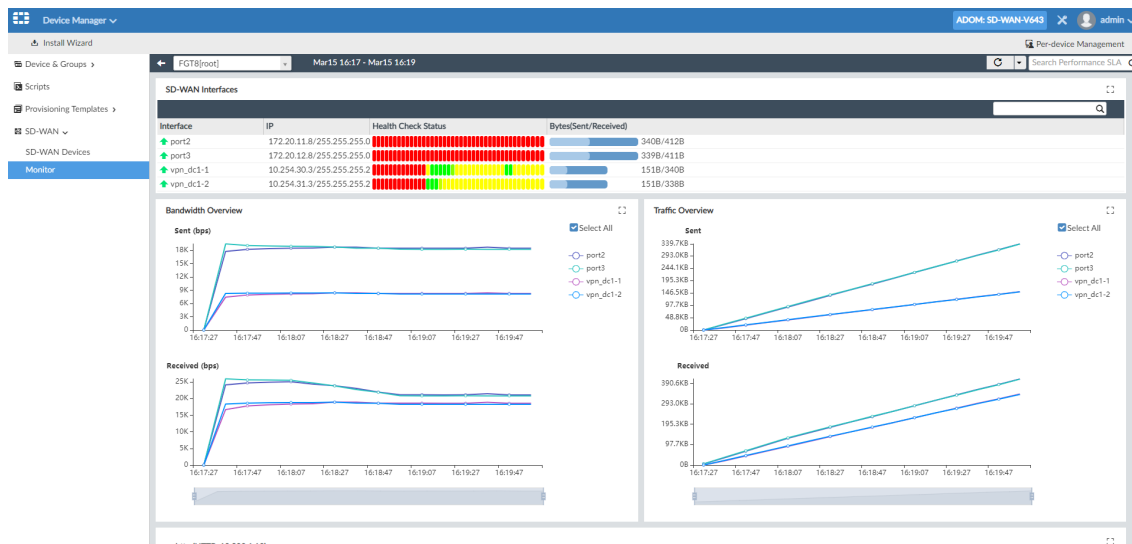
Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
Up	DC4-FGT[root]	vpn-br1-1_0	dialup	172.20.11.8	1d 23h 24m 38s	vpn-br1-1_p2	107.2 KB
Up	DC4-FGT[root]	vpn-br1-1_1	dialup	172.20.11.9	14d 4h 8m 14s	vpn-br1-1_p2	1.4 GB
Up	DC4-FGT[root]	vpn-br1-2_0	dialup	172.20.12.8	14d 4h 8m 14s	vpn-br1-2_p2	109.1 KB
Up	DC4-FGT[root]	vpn-br1-2_1	dialup	172.20.12.9	14d 4h 8m 13s	vpn-br1-2_p2	2.1 GB
Up	FGT8[root]	vpn_dcl-1	automatic	172.20.10.7	54s	vpn_dcl-1_p2	123.9 KB
Up	FGT8[root]	vpn_dcl-2	automatic	172.20.9.7	54s	vpn_dcl-2_p2	126.1 KB
Up	FGT9[root]	vpn_dcl-1	automatic	172.20.10.7	13d 12h 34m 54s	vpn_dcl-1_p2	1.8 GB
Up	FGT9[root]	vpn_dcl-2	automatic	172.20.9.7	13d 12h 34m 54s	vpn_dcl-2_p2	2.5 GB

To view SD-WAN monitor:

1. Disable device history monitoring by using the following command:

```
config system admin setting
    set sdwan-monitor-history disable
end
```

2. Go to **Device Manager > Monitors > SD-WAN Monitor**.
The **SD-WAN Monitor** is displayed.
3. In the toolbar, click **Table View**.
Table View is displayed.
4. In the **Device** column, click a device.
SD-WAN monitoring information for the last 10 minutes for the device is displayed. In the **SD-WAN Interfaces** section, you can view interfaces.



Scroll down to view SLA information, such as latency, jitter, and packet loss.



Monitoring SD-WAN interfaces (with shortcuts)

When an SD-WAN network is configured to use ADVPN shortcuts, you can view information about the shortcuts on **VPN Monitor** and in graphs on **SD-WAN Monitor**.

In this example, device history monitoring is enabled for **SD-WAN Monitor**.

To view shortcut information on VPN monitor:

1. Go to *Device Manager > Monitors > VPN Monitor*.
The *VPN Monitor* is displayed. Shortcuts are configured.

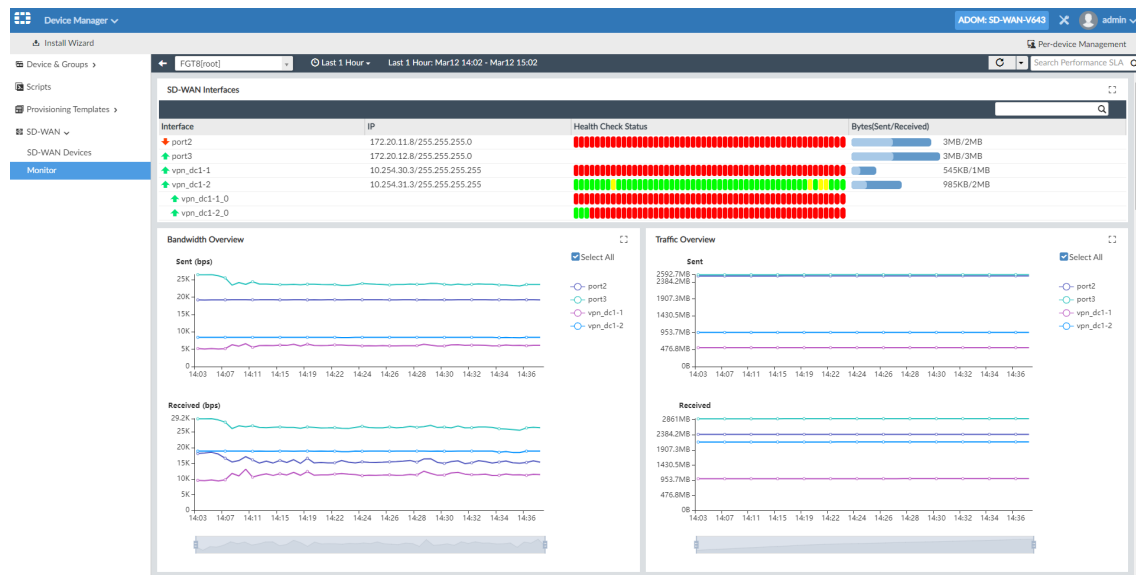
Status	Device	P1 Name	Type	Remote Gateway	Uptime	P2 Name	Incoming Data
Up	DC4-FGT[root]	vpn-br1-1_0	dialup	172.20.11.8	1d 4h 14m 57s	vpn-br1-1_p2	192.8 MB
Up	DC4-FGT[root]	vpn-br1-1_1	dialup	172.20.11.9	13d 8h 58m 33s	vpn-br1-1_p2	1.3 GB
Up	DC4-FGT[root]	vpn-br1-2_0	dialup	172.20.12.8	13d 8h 58m 33s	vpn-br1-2_p2	197.1 MB
Up	DC4-FGT[root]	vpn-br1-2_1	dialup	172.20.12.9	13d 8h 58m 33s	vpn-br1-2_p2	2.0 GB
Up	FGT8[root]	vpn_dc1-1	automatic	172.20.10.7	1d 4h 15m 18s	vpn_dc1-1_p2	222.2 MB
Up	FGT8[root]	vpn_dc1-1_0	dialup	172.20.11.9	02m 00s	vpn_dc1-1_p2	75.9 KB
Up	FGT8[root]	vpn_dc1-2	automatic	172.20.9.7	1d 4h 52m 38s	vpn_dc1-2_p2	227.2 MB
Up	FGT8[root]	vpn_dc1-2_0	dialup	172.20.12.9	01m 46s	vpn_dc1-2_p2	81.4 KB
Up	FGT9[root]	vpn_dc1-1	automatic	172.20.30.7	12d 18h 9m 25s	vpn_dc1-1_p2	1.7 GB
Up	FGT9[root]	vpn_dc1-1_0	dialup	172.20.11.8	02m 30s	vpn_dc1-1_p2	83.7 KB
Up	FGT9[root]	vpn_dc1-2	automatic	172.20.9.7	12d 18h 9m 25s	vpn_dc1-2_p2	2.3 GB
Up	FGT9[root]	vpn_dc1-2_0	dialup	172.20.12.8	01m 46s	vpn_dc1-2_p2	81.4 KB

To view shortcut information on SD-WAN monitor:

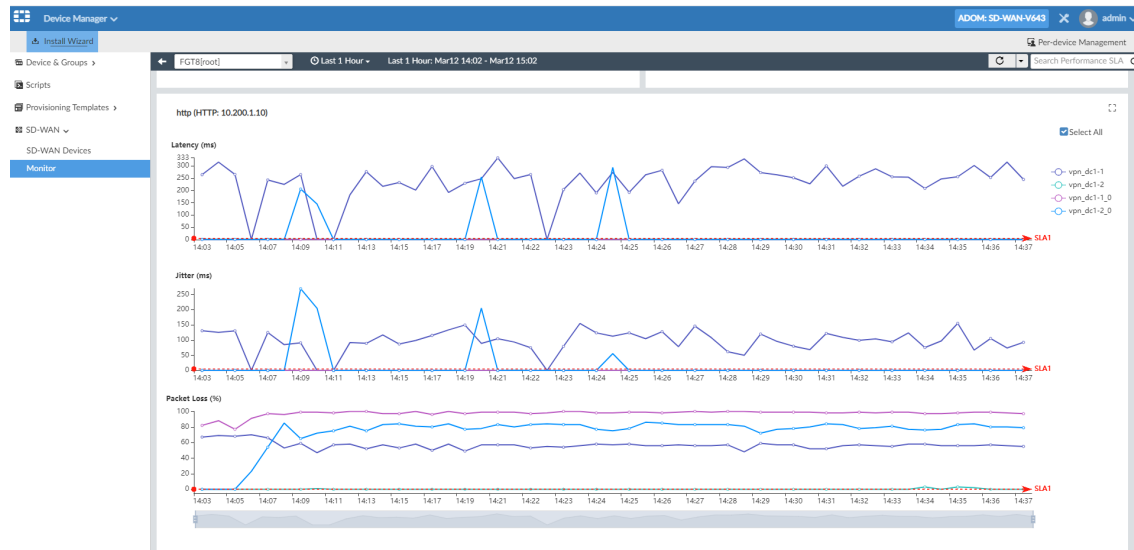
1. Enable device history monitoring by using the following command:

```
config system admin setting
set sdwan-monitor-history enable
end
```
2. Go to *Device Manager > Monitors > SD-WAN Monitor*.
The *SD-WAN Monitor* is displayed.
3. In the toolbar, click *Table View*.
Table View is displayed.
4. In the *Device* column, click a device.

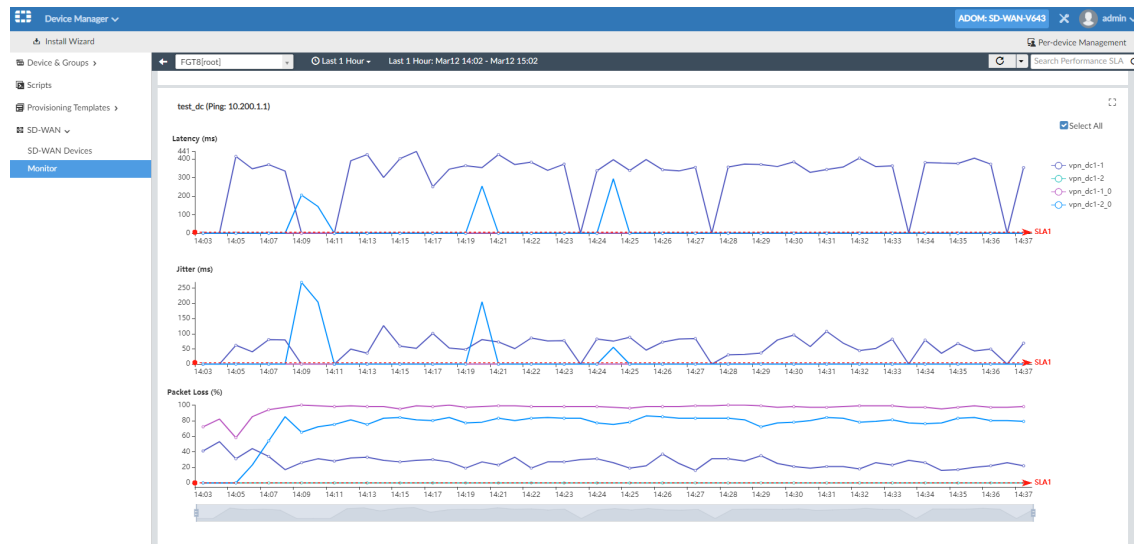
SD-WAN monitoring information for the device is displayed. You can choose the length of history to display. In the *SD-WAN Interfaces* section, you can view interfaces, including ADVPN shortcuts.



Scroll down to view SLA information, such as latency, jitter, and packet loss, for each interface. The SLA graphs include information for dynamic interfaces.



Scroll down to view more interfaces.



Templates

This section lists the new features added to FortiManager for templates:

- [Interface template support for meta fields on page 35](#)
- [Static route template with support for meta fields on page 40](#)
- [Pre-defined IPsec template with recommended settings on page 45](#)
- [Un-assign IPsec template to remove VPN-related configuration on page 47](#)
- [IPsec template enhanced support for tunnel interface configuration 7.0.1 on page 51](#)
- [CLI Template improvements 7.0.1 on page 48](#)
- [Templates support assignment to device groups 7.0.1 on page 53](#)

Interface template support for meta fields

When you create a meta field for a device object, a variable name is automatically created, and you can use the variable in interface templates when provisioning FortiGates.

When you create a meta field, you can specify whether it is required or optional. When the meta field is required for device objects, you must define a value for all FortiGate devices. A column is automatically displayed on the *Device Manager* pane to indicate required meta fields and to help you identify when values are missing.

After you assign interface templates to devices, you can view the post action values before you install the configuration to devices.

This topic includes the following sections:

- [Creating meta field variables on page 35](#)
- [Using meta field variables in interface templates on page 36](#)
- [Viewing required meta fields in Device Manager on page 37](#)
- [Assigning interface templates to devices on page 38](#)
- [Overriding meta field values in interface templates on page 39](#)

Creating meta field variables

When you create a meta field, a variable name is automatically created, and you can set a value for the variable for each device.

This example describes how to create a meta field named *storenumber* for a device object. The *storenumber* meta field is set to *Required*. When a meta field is set to *Required*, a value must be defined for all devices. Set the meta field to *Optional* to avoid this requirement.

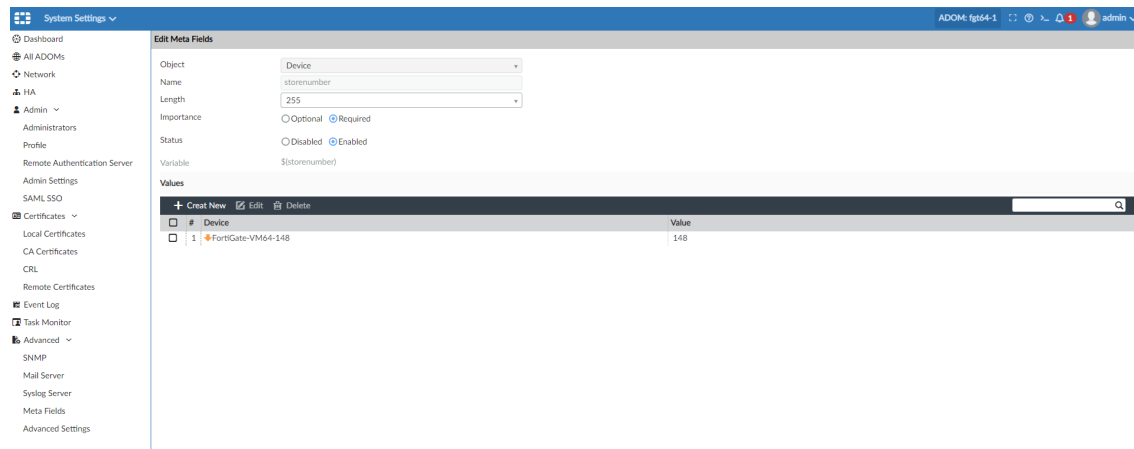
To create meta field variables:

1. Go to *System Settings > Advanced > Meta Fields*, and click *Create New*.
The *Create New Meta Fields* dialog box is displayed.
2. In the *Object* list, select *Device*.
3. In the *Name* box, type `storenumber`.

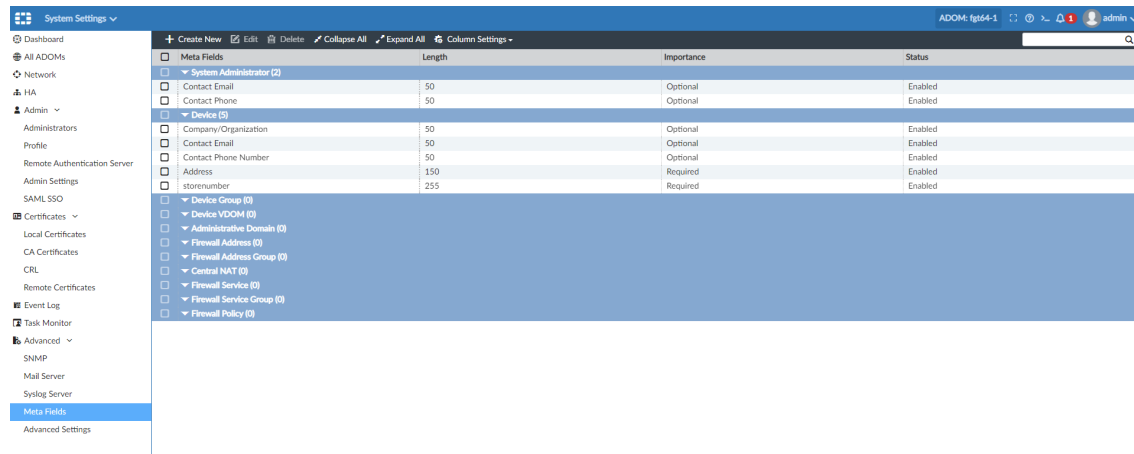


The name identifies the meta field, and a variable name is automatically created for the meta field. View the *Variable* option to see the variable name that you can use in interface templates. For example, `$(storenumber)` is the variable name for the *storenumber* meta field.

4. Beside *Importance*, select *Required*.
5. Define the value:
 - a. Under *Values*, click *Create New*.
The *Create Meta Field Value* dialog box is displayed.
 - b. In the *Device* list, select the device.
 - c. In the *Value* box, type the store number.
 - d. Click *OK*.
The value is saved.



- Click **OK**.
The meta field is created.



Using meta field variables in interface templates

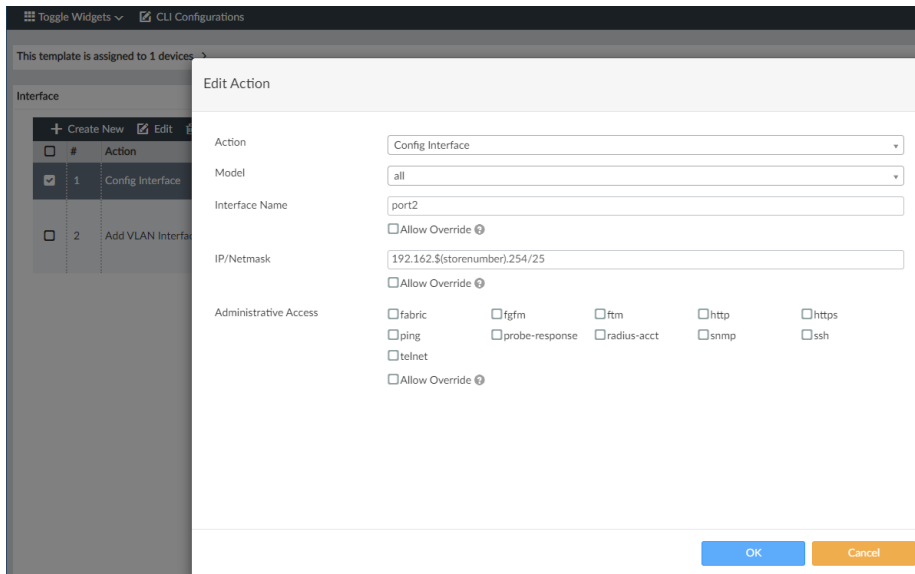
You can use meta field variables in interface templates. When you create a meta field, a variable is automatically created for you. You can use the variable in interface templates.

To use meta field variables in interface templates:

- Go to *Device Manager > Provisioning Templates*.
The widgets are displayed.
- Display the *Interface* widget.
 - In the tree menu, go to *System Templates > Default*.
 - From the *Toggle Widgets* menu, select *Interface*.
The *Interface* widget is displayed.
- In the *Interface* widget, create a new *Config Interface* action that uses the *storenumber* variable.
 - In the *Interface* widget, click **+**.
 - In the *Action* list, select *Config Interface*.
 - In the *Model* list, select *all*.
 - In the *Interface Name* list, type `port2`.

- e. In the *IP/Netmask* box, type the variable with the IP/netmask, such as `192.162. $(storenumber) .254/25`, and click **OK**.

Note that `$(storenumber)` is the variable name for the meta field.



The action is created.

4. In the *Interface* widget, create a new *VLAN Interface* action that uses the variable.
 - a. In the *Interface* widget, click **+**.
 - b. In the *Action* list, select *Add VLAN Interface*.
 - c. In the *Model* list, select *all*.
 - d. In the *Physical Interface Name* list, type `port3`.
 - e. In the *VLAN Name* box, type the variable name, such as `$(Address)`, and click **OK**.

The action is created.

Viewing required meta fields in Device Manager

When a meta field is required for devices, you must assign an interface template to devices. If a device lacks a meta field value, a conflict symbol is displayed, and you cannot assign an interface template to it. You must define a value for the meta field for the device before you can assign an interface template to it.

To view required meta fields in Device Manager:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, click *Managed Devices*.

The managed devices are displayed in the content pane. A column is displayed for each required meta field. In the following example, a column for each of the following required meta fields is displayed: *Address* and *storenumber*.

A conflict symbol is displayed for *storenumber* for one of the FortiGates, indicating that a value is not defined for the meta field for the device.

The screenshot shows the FortiManager Device Manager interface. At the top, there are tabs for 'Device Manager', 'Device & Groups', 'Firmware', 'License', 'Provisioning Templates', 'Scripts', and 'SD-WAN'. Below these, there's a 'Managed Devices' section with a table of devices. The table has columns for 'Device Name', 'Package Status', 'Firmware Version', 'Host Name', 'IP Address', 'Platform', 'Description', 'Address', and 'storenumber'. Two devices are listed: 'FortiGate-VM64-148' and 'FortiGate-VM64-149'. Both are marked as 'Installed'. The 'FortiGate-VM64-149' device has a red conflict icon in the 'storenumber' column.

Device Name	Package Status	Firmware Version	Host Name	IP Address	Platform	Description	Address	storenumber
FortiGate-VM64-148	Installed	FortiGate 6.4.3.build1778 (Interim)	FortiGate-VM64	10.2.114.148	FortiGate-VM64		add-148	148
FortiGate-VM64-149	Installed	FortiGate 6.4.2.build1723 (GA)	FortiGate-VM64	10.2.114.149	FortiGate-VM64		add-149	149

Assigning interface templates to devices

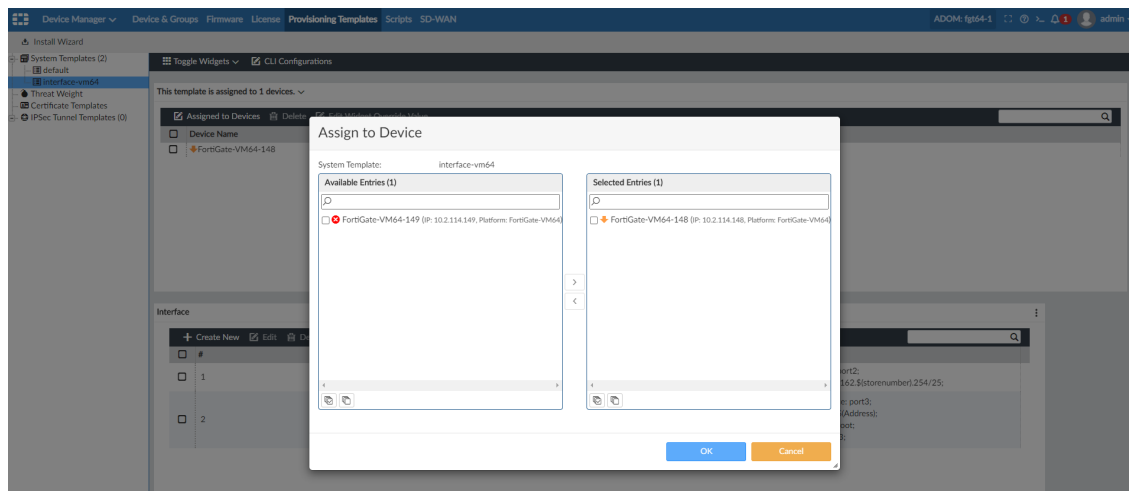
You must assign an interface template to devices when *Required* is enabled for certain meta fields.

You can also preview the meta field value.

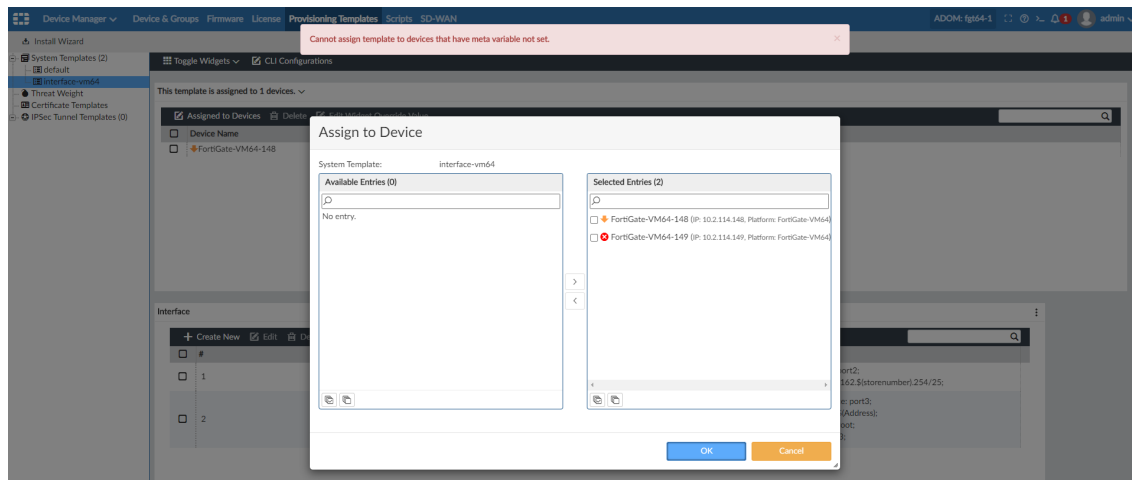
To assign interface templates to devices:

1. Go to *Device Manager > Provisioning Templates*, and select the template.
2. In the content pane, expand *This template is assigned to <number> devices*.
3. Click *Assigned to Devices*.
4. In the *Available Entries* list, select the device, and click *>* to move it to the *Selected Entries* list. Click *OK*. The interface template is assigned to the device.

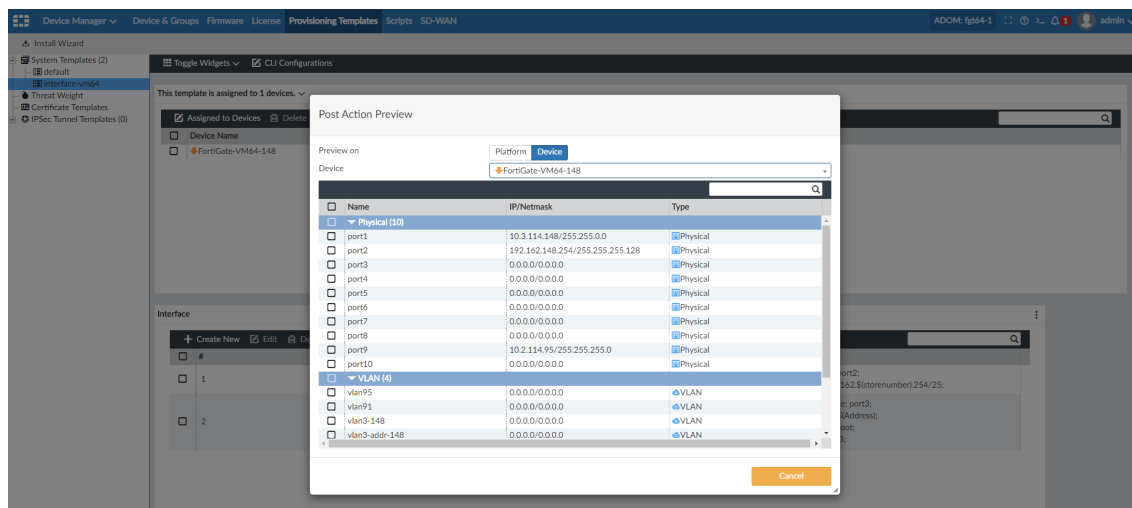
When a FortiGate lacks a value for a meta field, a red conflict icon is displayed:



When you try to assign the template, an error message is displayed:



5. In the *Interface* widget, select the action, and click *Post Action View*.
The *Post Action Preview* is displayed. The meta field displays the expected value.



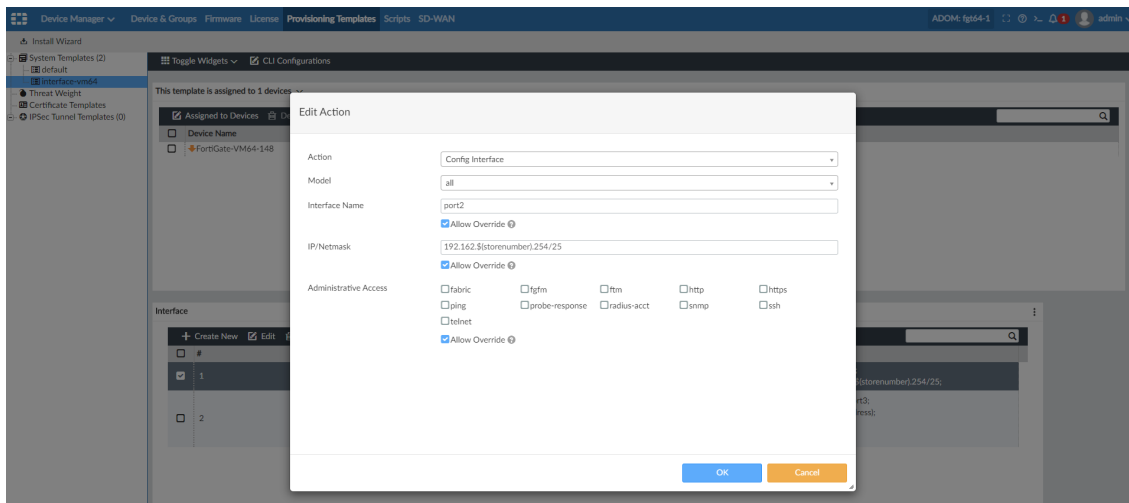
6. Click *Cancel*.

Overriding meta field values in interface templates

You can enable *Allow Override* in interface templates for some options. After you assign the interface template to a device, you can edit the interface action to override the option.

To override meta field values in interface templates:

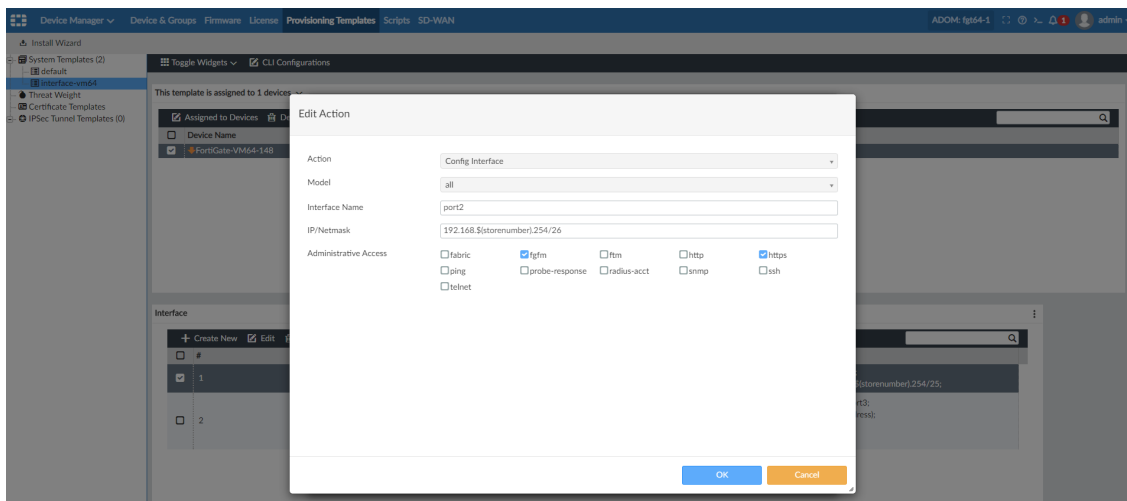
1. Go to *Device Manager > Provisioning Templates*, and select the template.
2. Edit the interface template to allow overrides.
 - a. In the *Interface* widget, select the action, and click *Edit*.
 - b. Under the option, select *Allow Override*, and click *OK*.
Overrides are allowed for the option.



3. Override the value.

- a. Under *This template is assigned to <number> devices* widget, select the device, and click *Edit Widget Override Value*.

The *Edit Action* dialog box is displayed.



- b. Type the override value, and click *OK*.

4. Install the configuration to the device.

The override value is installed to the device.

Static route template with support for meta fields

You can provision static routes to FortiGate devices by using a static route template. Both IPv4 and IPv6 are supported. After creating the static route template, you can assign the template to one or more devices, and install the configuration to devices.

For IPv4, you can create static routes for the following destinations:

- Subnet
- Internet service
- Custom Internet service

You can use meta field variables created for an object type of *Device VDOM* when creating IPv4 static routes for subnets.

Edit Static Route

To use meta field, the input format is \$(meta_field_name).

Type

IPv4 IPv6

Destination

Subnet Internet Service Internet Service Custom

Gateway Address

\$(vdom-ip)/255.255.255.0

Interface

port5

Administrative Distance

10

Comments

Status

ON

Advanced Options >

For IPv6, you can create a static route:

Create New Static Route

To use meta field, the input format is \$(meta_field_name).

Type

IPv4 IPv6

Destination

::/0

Gateway Address

::

Interface

Administrative Distance

10

Comments

Status

ON

Advanced Options >

OK

Cancel

This topic contains the following sections:

- [Creating meta field variables on page 41](#)
- [Creating static route templates on page 42](#)

Creating meta field variables

You can create meta field variables for an object type of *Device VDOM*, and then use the variable in static route templates.

When you create a meta field, a variable name is automatically created, and you can set a value for the variable for each device.

This example describes how to create a meta field named *vdom-ip* for a *Device VDOM* object.

To create meta field variables:

1. Go to *System Settings > Advanced > Meta Fields*, and click *Create New*.
The *Create New Meta Fields* dialog box is displayed.
2. In the *Object* list, select *Device VDOM*.
3. In the *Name* box, type *vdom-ip*.



The name identifies the meta field, and a variable name is automatically created for the meta field. View the *Variable* option to see the variable name that you can use in interface templates. For example, *\$(vdom-ip)* is the variable name for the *vdom-ip* meta field.

4. Beside *Importance*, select *Required*.
5. Define the value:
 - a. Under *Values*, click *Create New*.
The *Create Meta Field Value* dialog box is displayed.
 - b. In the *Device* list, select the device.
 - c. In the *Value* box, type the IP address.
 - d. Click *OK*.
The value is saved.

#	Device	Value
1	FGT-VM64-154(root)	192.168.111.154
2	FGT-VM64-155(vn1-profile)	192.168.111.155
3	FGT-VM64-155(root)	192.168.111.155

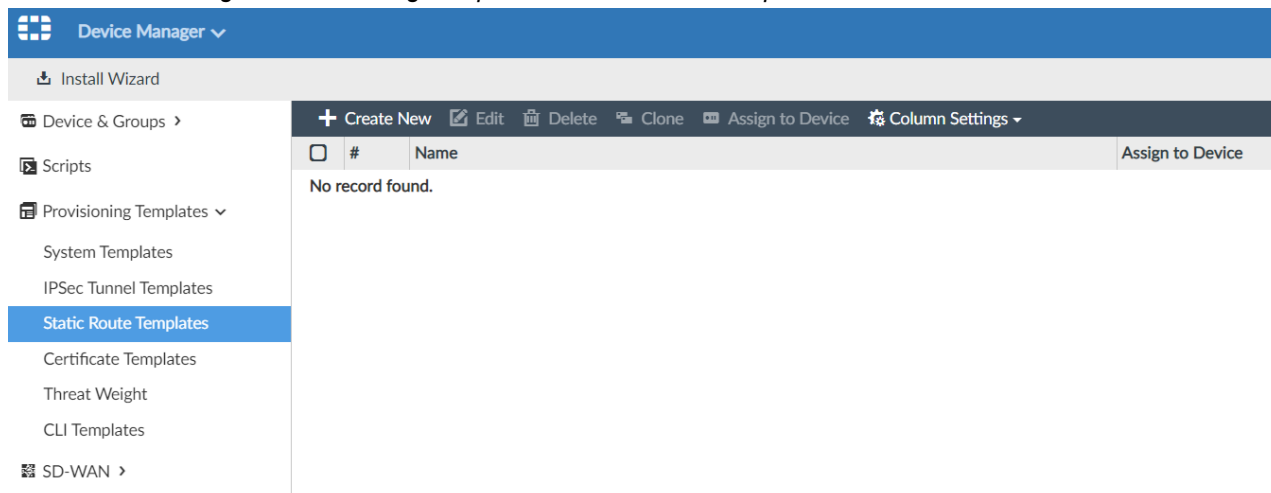
6. Click *OK*.
The meta field is created.

Creating static route templates

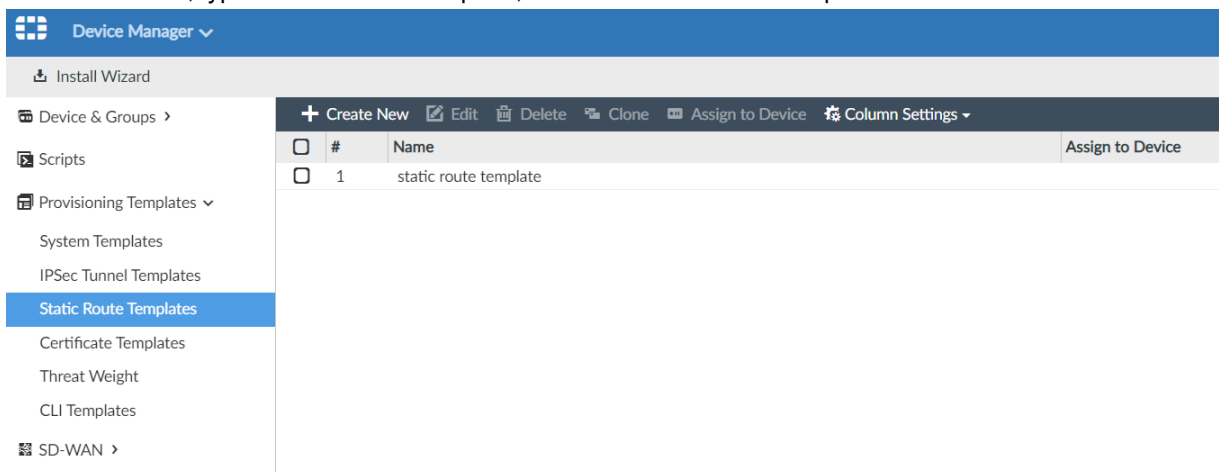
You can use meta field variables created for an object type of *Device VDOM* when creating IPv4 static routes for subnets.

To create a new static route template:

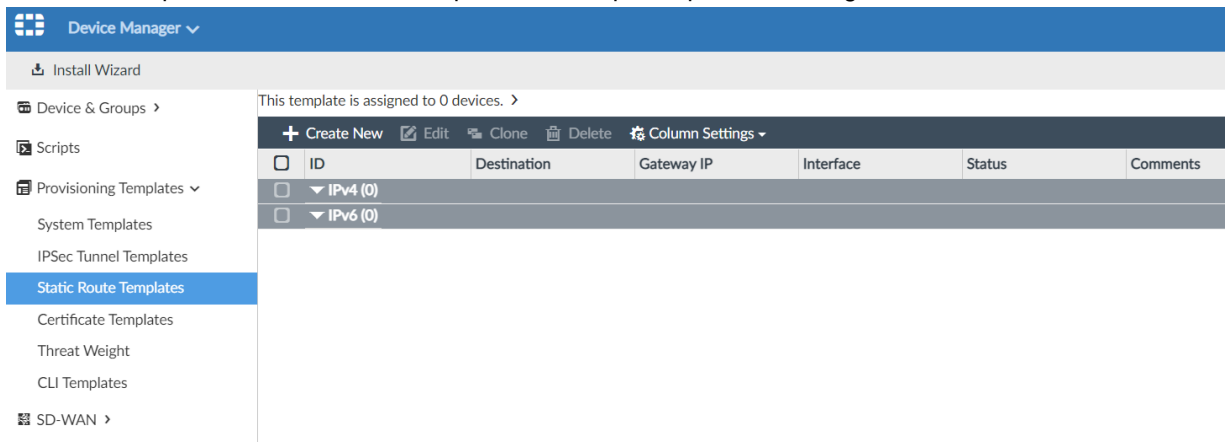
1. Go to *Device Manager > Provisioning Templates > Static Route Templates*.



2. Create a static route template:
 - a. In the toolbar, click *Create New*. The *Create New Route Template* dialog box appears.
 - b. In the *Name* box, type a name for the template, and click *OK*. The new template is created.



3. Open the template for editing, and create a static route:
 - a. In the content pane, double-click the template. The template opens for editing.



- b. In the toolbar, click *Create New*. The *Create New Static Route* pane is displayed. For IPv4 subnets, you can use a meta field variable created for an object type of *Device VDOM* instead of typing an IP address. For example:

The screenshot shows the "Create New Static Route" dialog box. At the top, a message box states: "To use meta field, the input format is \${meta_field_name}." Below this, the form has the following fields and options:

- Type:** Radio buttons for IPv4 (selected) and IPv6.
- Destination:** Radio buttons for Subnet (selected), Internet Service, and Internet Service Custom.
- Gateway Address:** Text input field with the value "0.0.0.0/0.0.0.0".
- Interface:** Text input field with the value "0.0.0.0".
- Administrative Distance:** Text input field with the value "10".
- Comments:** Text area with a character count of "0/255".
- Status:** Toggle switch set to "ON".
- Advanced Options:** A link to expand more options.

At the bottom right of the dialog are "OK" and "Cancel" buttons.

- c. Complete the options, and click *OK*.
The static route is created.
4. Assign the template of static routes to one or more devices.
5. Install the configuration to devices.

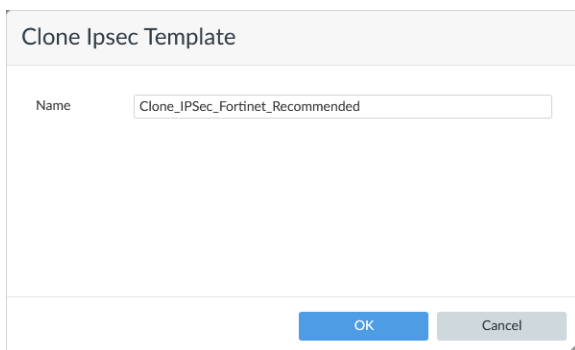
Pre-defined IPsec template with recommended settings

FortiManager includes a default IPsec template called *IPSec_Fortinet_Recommended*. The default template contains recommended VPN tunnel settings and best practices. You can clone the template and customize settings in the clone to create new IPsec templates.

After editing the cloned template, assign the template to devices. When you install the settings to devices, phase1/phase2 interface settings are installed to devices.

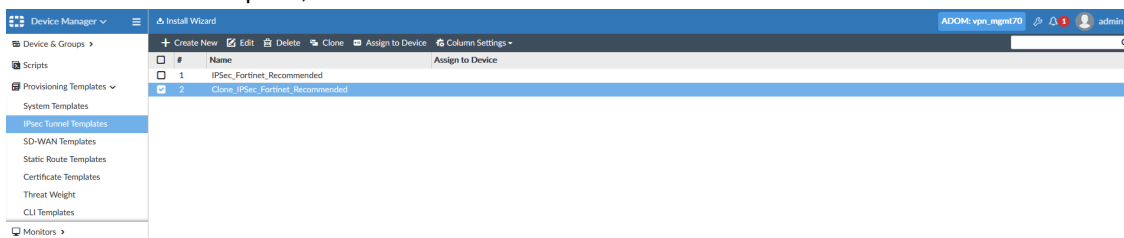
To use the default IPsec template:

1. Go to *Device Manager > Provisioning Templates > IPsec Tunnel Templates*.
The templates are displayed in the content pane, including the *IPSec_Fortinet_Recommended* template.
2. Clone the *IPSec_Fortinet_Recommended* template:
 - a. Select the *IPSec_Fortinet_Recommended* template, and click *Clone*.
The *Clone IPsec Template* dialog box is displayed.



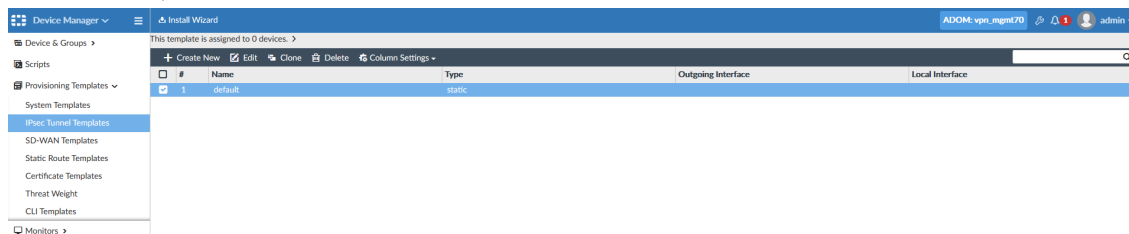
The dialog box titled "Clone IPsec Template" has a "Name" field containing the text "Clone_IPSec_Fortinet_Recommended". At the bottom right, there are "OK" and "Cancel" buttons.

- b. In the *Name* box, type a name for the cloned template, and click *OK*.
The cloned template is displayed in the content pane.
- c. Select the cloned template, and click *Edit*.



The cloned template opens for editing. The cloned template includes default tunnel settings named *default*.

3. Select *default*, and click *Edit*.



The default tunnel settings open for editing.

4. Edit the tunnel settings, and click **OK** to save the changes.
5. Assign the template to one or more devices:
 - a. Click *IPsec Tunnel Templates* to display all templates.
 - b. Select the template, and click *Assign to Device*.
The *Assign to Device* dialog box is displayed.

- c. In the *Available Entries* list, select devices, and click **>** to move them to the *Selected Entries* list, and click **OK**.
The template is assigned to the devices in the *Selected Entries* list and ready for use.
6. Install device settings to install phase1/phase2 interface configuration to devices.

Un-assign IPsec template to remove VPN-related configuration

When you un-assigning an IPsec template from a device, FortiManager modifies the configuration for affected devices. When you install the modified configuration to devices, FortiManager automatically uninstalls the configuration (phase1/phase2 interfaces) generated by the IPsec template from devices.

This topic describes how you can view the changes in the FortiManager GUI.

To view how un-assigned IPsec templates affect devices:

1. Create an IPsec template named *toHQ-1*, and install it to devices.

After installing the IPsec template, go to *Device Manager > Device & Groups*, and select *Table View*. In the *Config Status* column, view a status of *Synchronized* for all affected devices, and the *Provisioning Templates* column shows that the *toHQ-1* template has been applied.

Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Version
vlan171_0091	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0066 (GA)
vlan171_0092	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0066 (GA)
vlan171_0093	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0057 (Interim)
root [NAT] (Management)	Synchronized	default		
SIMPLY-ENERGY [NAT]	Synchronized	default		
vd_1 [NAT]	Synchronized	default	toHQ-1	
vlan171_0094	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0057 (Interim)
root [NAT] (Management)	Synchronized	default		
vd_1 [NAT]	Synchronized	default	toHQ-1	
vlan171_0095	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0057 (Interim)
root [NAT] (Management)	Synchronized	default		
FG-traffic [NAT]	Synchronized	default	toHQ-1	
vlan171_0096	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0057 (Interim)
vlan171_0097	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0057 (Interim)
vlan171_0098	Synchronized	default	toHQ-1	FortiGate 7.0.0.build0057 (Interim)

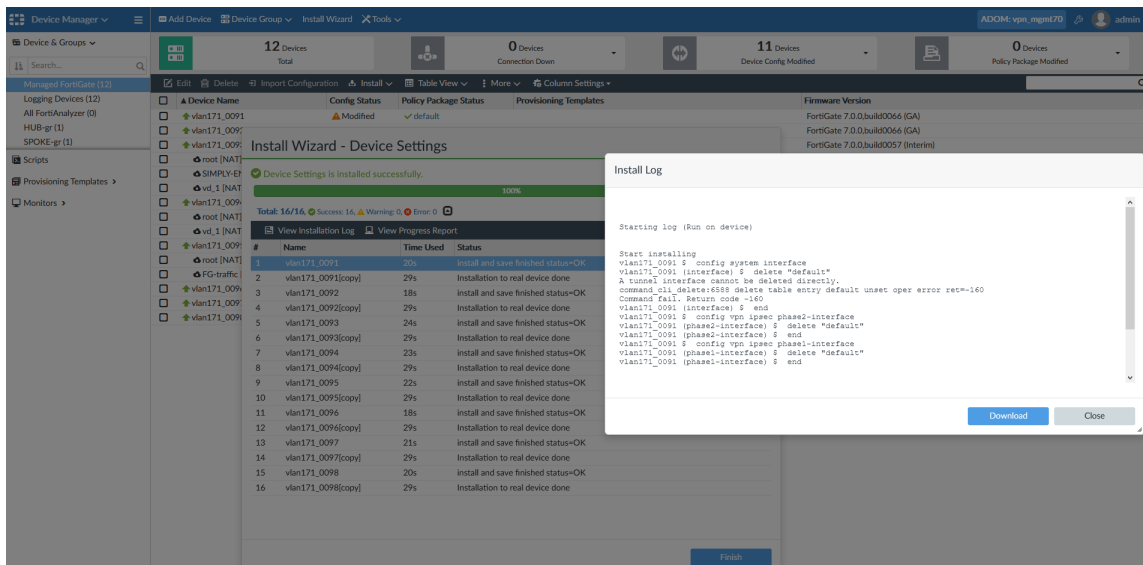
2. Un-assign the IPsec template from eight devices.

After un-assigning the *toHQ-1* template from eight devices, the *Config Status* column now shows a status of *Modified* for all devices, and the *Provisioning Templates* column no longer displays the *toHQ-1* template.

Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Version
vlan171_0091	Modified	default		FortiGate 7.0.0.build0066 (GA)
vlan171_0092	Modified	default		FortiGate 7.0.0.build0066 (GA)
vlan171_0093	Modified	default		FortiGate 7.0.0.build0057 (Interim)
root [NAT] (Management)	Synchronized	default		
SIMPLY-ENERGY [NAT]	Synchronized	default		
vd_1 [NAT]	Modified	default		
vlan171_0094	Modified	default		FortiGate 7.0.0.build0057 (Interim)
root [NAT] (Management)	Synchronized	default		
vd_1 [NAT]	Modified	default		
vlan171_0095	Modified	default		FortiGate 7.0.0.build0057 (Interim)
root [NAT] (Management)	Synchronized	default		
FG-traffic [NAT]	Modified	default		
vlan171_0096	Modified	default		FortiGate 7.0.0.build0057 (Interim)
vlan171_0097	Modified	default		FortiGate 7.0.0.build0057 (Interim)
vlan171_0098	Modified	default		FortiGate 7.0.0.build0057 (Interim)

3. Install the modified device configuration to the devices.

FortiManager removes phase1 and phase2 interface configuration from the devices. You can check the *Install Log* for affected devices to confirm that FortiManager removed phase2 and phase1 interfaces settings.



CLI Template improvements - 7.0.1

In FortiManager 7.0.1, CLI templates include the following improvements:

- Jinja2 language support
- Validation check and preview
- Device and device-VDOM meta variables

To create an IPsec VPN using Jinja in the CLI Template:

1. Create a new meta field in FortiManager.
 - a. Go to *System > Advanced > Meta Fields* and create a new meta field.
 - b. Enter a name for the meta field, for example *outgoing_int*.
 - c. Enter the meta field object. In this example, the *Object* can be *Device* or *DeviceVDOM*.
 - d. Click OK.

Create New Meta Fields

Object: Device

Name: outgoing_int

Length: 20

Importance: ☒ Optional ☐ Required

Status: ☐ Disabled ☒ Enabled

Variable: \${outgoing_int}

Values

+ Create New Edit Delete

#	Device	Value
No record found.		

2. Create the CLI Jinja Template:
 - a. Go to *Device Manager > Provisioning Templates > CLI Template*, and create a new *CLI Template*.
 - b. Enter a name for the template, for example *IPSEC_VPN*.
 - c. Select *Jinja Script* as the *Type*.

- d. Enter the *Script Details*. In this example, the following jinja script is used to create the IPsec phase1-interface and phase 2-interface. Jinja2 uses {{ ... }} for the expression of variables.

```
config vpn ipsec phase1-interface
edit tohub1
set remote-gw 101.71.49.4
set interface {{ outgoing_int }}
set peertype any
set proposal aes128-sha256
set psksecret fortinet
next
end
config vpn ipsec phase2-interface
edit tohub1
set phase1name tohub1
set proposal aes128-sha256
set auto-negotiate enable
next
end
```

- e. Click OK.

The screenshot shows the 'Create New CLI Template' window in FortiManager. The left sidebar has 'Provisioning Templates' expanded, with 'CLI Templates' selected. The main area contains the following fields:

- Template Name: IPSEC_VPN
- Type: Jinja Script
- Comments: (empty text area)
- Script details: A text area containing the Jinja2 script for configuring IPsec phase1 and phase2 interfaces.

At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Assign a port to the new meta field.

- a. Go to *Device Manager* and edit your device.
- b. In the previously created meta field, enter a port. In this example, *port2* is assigned to the *outgoing_int* field.

The screenshot shows the 'Meta Fields' section in FortiManager. It lists several meta fields with their corresponding input boxes and required/optional status:

Meta Fields	Value	Required/Optional
Company/Organization		Optional
Contact Email		Optional
Contact Phone Number		Optional
Address	Kingsway 2700, Vancouver, British Columbia, Canada	Required
color		Required
outgoing_int	port2	Optional

4. Assign the CLI Jinja template to a device and execute device installation. The following configuration is pushed to the FortiManager.

```

config vpn ipsec phase1-interface
edit tohub1
    set remote-gw 101.71.49.4
    set interface port2
    set peertype any
    set proposal aes128-sha256
    set psksecret ENC
        Z8Zpc61yyxOe2K5QsJbYr7gRiykPe0EjU+e+TlSz12BucSSA6DfXPd23wnhkb560RSK92hqBpFH
        tC3/glfopSKt80jn1G+I/0YMlNty6aoiyrDx5duo0g5cL4rB7UuT8TmmyeCDeUVy5wyT4afglm5
        P9Q8IzkY2P3D5/FG5DIuYHMZZg
    next
end
config vpn ipsec phase2-interface
edit tohub1
    set phase1name tohub1
    set proposal aes128-sha256
    set auto-negotiate enable
next
end

```

To validate a CLI Template:

1. Go to *Device Manager > Provisioning Templates > CLI Template*.
2. Once the template is assigned to a device, click *Validate*.

Name	Type	Assigned Devices/Groups	Variables	Comments
CLI Template (8)				
001.IPSEC_VPN	Jinja		overlay1port overlay2port	
002.tunnel-IP	Jinja		branchID	
003_bgp	Jinja		branchID	
003_static_route11	CLI			
004_sdwan	Jinja			
IPSEC_VPN	Jinja	Branch1 (root)	outgoing_int	
test	Jinja		color	
test123	Jinja		REGION	
CLI Template Group (1)				
spoke	CLI/Jinja			

If there are any errors, for example missing values for meta fields, you can click *View Validation Result*.

#	Name	Time Used	Status
1	Branch1	2s	meta variables missed

[View Validation Result](#)

You will have the opportunity to input the value for the missing meta fields in the dialog box.

Validation Result - IPSEC_VPN

Device Name	outgoing_int
Branch1 [root]	port2

*Click metafield to edit is support in the table.

Close

To preview a CLI Template script:

1. Go to *Device Manager > Provisioning Templates > CLI Template*.
2. Once the template is assigned, click *Validate*.
3. Click *View Validation Result* when the script validation is completed, and then click *Preview Result*.
The CLI Template is replaced with the value or values seen by the end user. For example, in the example below the variable `{{outgoing_int}}` is replaced by `port2` in the script.

Validation Result - IPSEC_VPN

Device Name	outgoing_int
Branch1 [root]	port2 (from device)

*Click metafield to edit is support in the table.

Preview CLI Template IPSEC_VPN [Branch1 - root]

```

1: config vpn ipsec phase1-interface
2:   edit tohub1
3:   set remote-gw 101.71.49.4
4:   set interface port2
5:   set peertype any
6:   set proposal aes128-sha256
7:   set psksecret ENC Z8Zpc61yyxOe2K5QsJbYr7gRiykPe0EjU+e+TLsz12BucSSA6DfXBdpywnhkb560RSK92hqBpFHTC3/g1fopSKt80jn1
8:   next
9: end
10:
11: config vpn ipsec phase2-interface
12:   edit tohub1
13:   set phase1name tohub1
14:   set proposal aes128-sha256
15:   set auto-negotiate enable
16:   next
17: end
18:

```

Download Close

IPsec template enhanced support for tunnel interface configuration - 7.0.1

IPSEC template enhanced support for tunnel interface configuration.

To configure an IPsec template:

1. Go to *Device Manager > Provisioning Template > IPsec Tunnel Templates*, and create or edit a template.
2. In the template, configure the IP address for an IPsec tunnel interface in Tunnel Interface Setup:
 - **IP:** Input the IP address, for example `10.10.1.1/32`. Meta fields are also supported, for example `10.10.$(side_id).1/32`.
 - **Remote IP:** Input the IP address or meta field for the remote IP.

The screenshot shows the 'Edit IPsec' configuration page in FortiManager. The left sidebar contains a navigation menu with the following items: Device & Groups, Scripts, Provisioning Templates (expanded), System Templates, IPsec Tunnel Templates (selected), SD-WAN Templates, Static Route Templates, Certificate Templates, Threat Weight, CLI Templates, NSX-T Service Template, Firmware Templates, and Monitors. The main content area is titled 'Edit IPsec' and includes the following fields and sections:

- Tunnel Name:** tohub
- Network:** Routing (Manual/Automatic)
- Remote Device:** IP Address/Dynamic DNS/Dynamic
- Remote Gateway (IP Address):** 10.7.10.159
- Outgoing Interface:** wan1
- Local Interface:** ipsecLAN
- Local Network Address Object Name:** internal_subnet
- Authentication:** Pre-shared Key/Signature
- Pre-shared Key:** (masked)
- Tunnel Interface Setup:**
 - IP:** 10.10.1.1/255.255.255.255
 - Remote IP:** 10.10.1.255/255.255.255.0
- Advanced Options:** (link)

3. Click **OK** to save the template.
4. Click **Install Wizard** at the top of the page to perform an installation.
The *Install Preview* shows that FortiManager is pushing the IPsec VPN tunnel interface and its IP address to the

device.

Install Preview of vlan171_0064

```

1: config global
2:   config system interface
3:     edit "tohub"
4:       set vdom "vd_1"
5:       set ip 10.10.1.1 255.255.255.255
6:       set type tunnel
7:       set remote-ip 10.10.1.255 255.255.255.0
8:       set snmp-index 115
9:       set interface "port2"
10:    next
11:  end
12: end
13: config vdom
14:   edit vd_1
15:     config vpn ipsec phase1-interface
16:       edit "tohub"
17:         set interface "port2"
18:         set comments "VPN: tohub [Created by IPSEC Template]"
19:         set wizard-type static-fortigate
20:         set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
21:         set peertype any
22:         set remote-gw 10.7.5.159
23:         set net-device disable
24:         set psksecret ENC Z8Zpc/bwU2j1HxCFsp0zLVsmpXEWQqvc6JVoYq8gt3RKcH0GzuPHQAo4U0l/tm1eYnZMKjWCX/cNxSUV
25:       next
26:     end
27:     config vpn ipsec phase2-interface
28:       edit "tohub"
29:         set phase1name "tohub"
30:         set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305

```

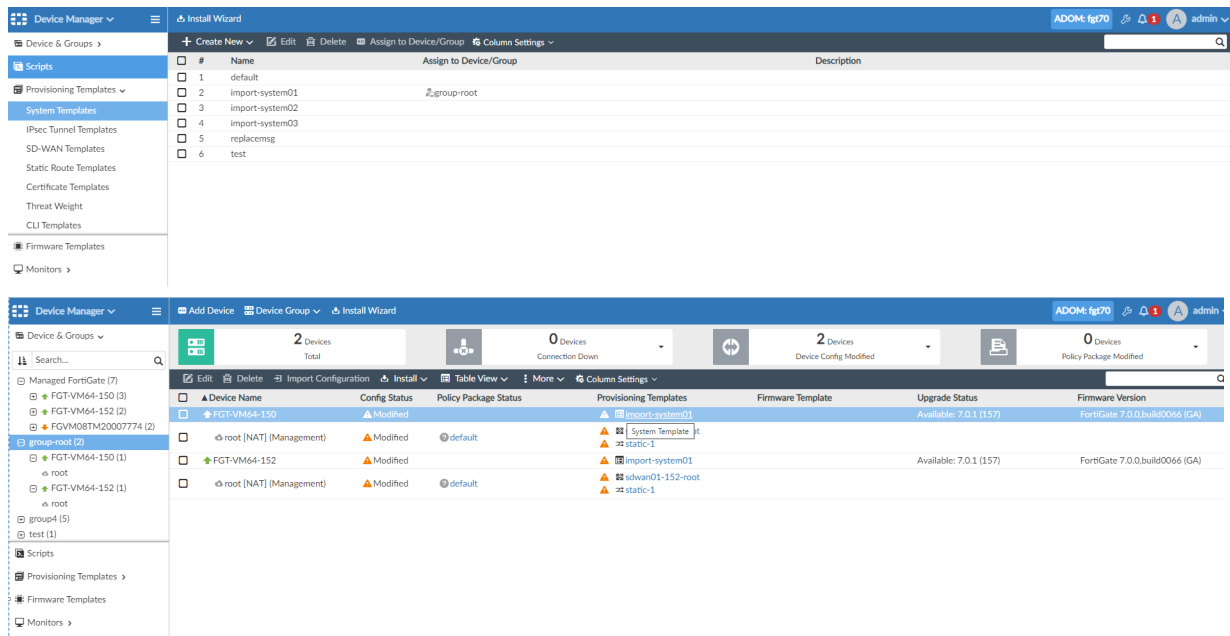
[Download](#)
[Close](#)

Templates support assignment to device groups - 7.0.1

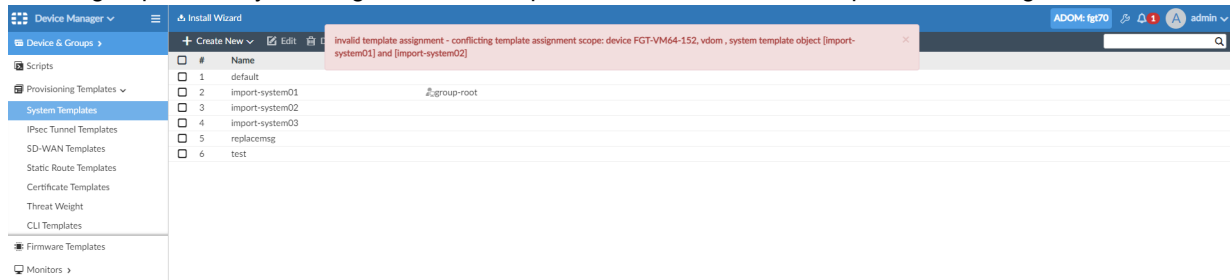
In FortiManager 7.0.1, templates support assignment to device groups.

To assign templates to a device group:

1. System Templates, SD-WAN Templates, Static Route Templates, and IPsec Templates can be assigned to a device or device group.



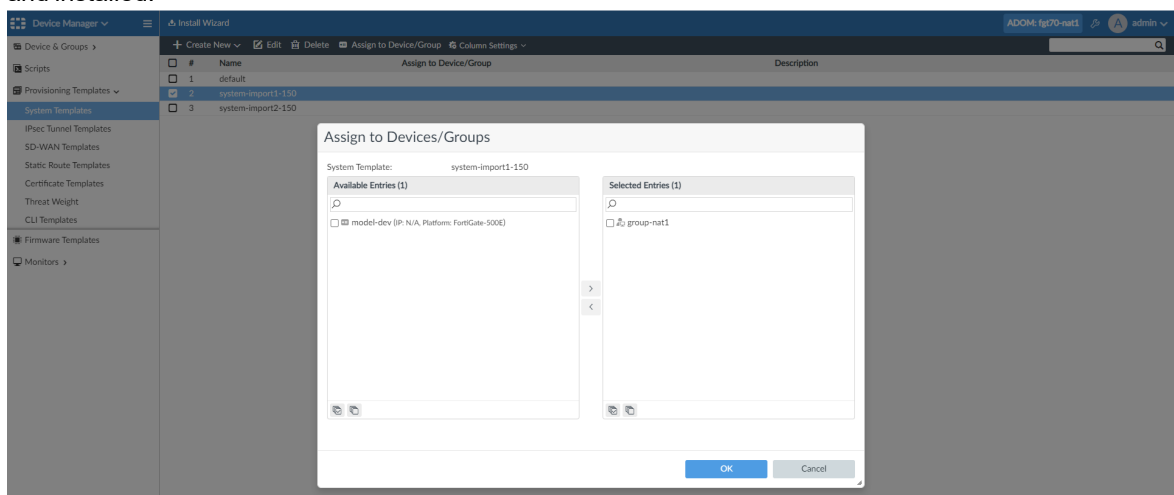
2. Device groups can only be assigned to one template, otherwise an error is reported indicating a conflict.



3. When assigning templates to device groups, the following applies:

a. System Template:

- For ADOMs with a management VDOM, templates can be assigned to the device group, then modified and installed.

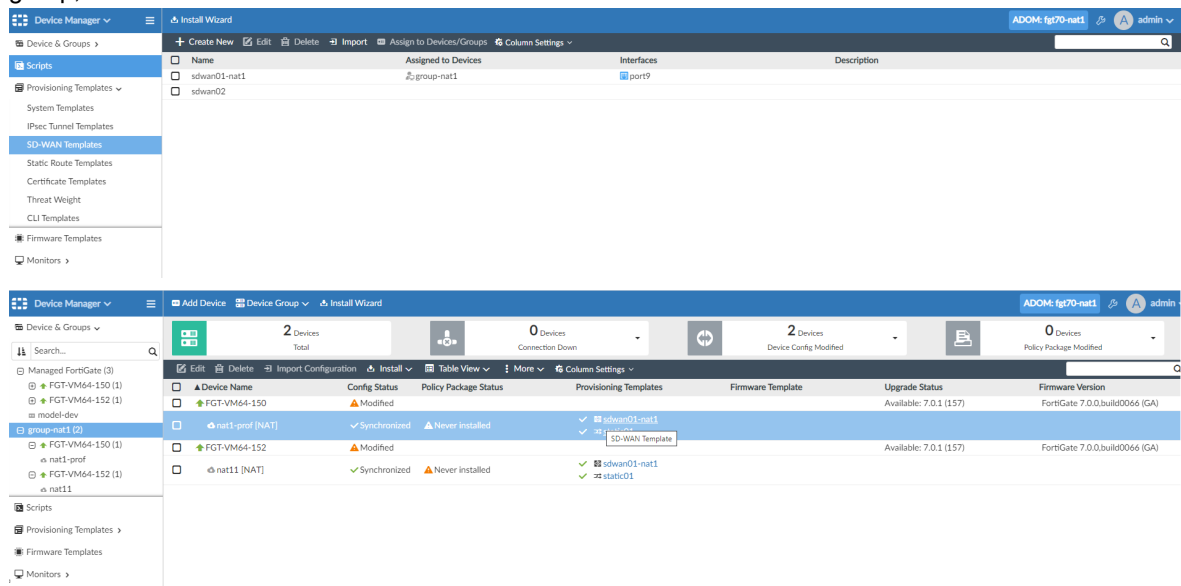


- For ADOMs with a non-management VDOM, the template cannot be assigned to the device group.



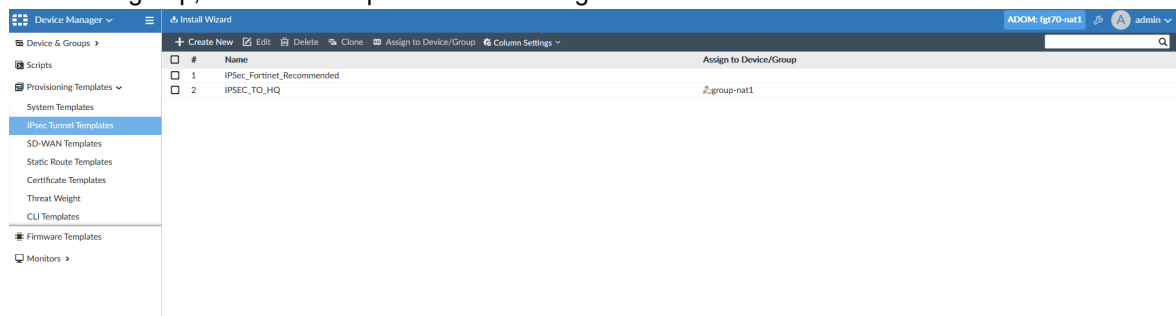
b. SD-WAN Template and Static Route Templates:

- For ADOMs with a management or non-management VDOM, templates can be assigned to the device group, then modified and installed.



c. IPsec Templates:

- IPsec Templates can be assigned to a device group. You can unassign an IPsec template from a device group member by going to *Device Manager* and editing the device group. When a device is removed from the device group, the IPsec Template will be unassigned from that device.



Firmware Upgrades

This section lists the new features added to FortiManager for firmware upgrades:

- [Firmware template on page 56](#)

Firmware template

You can create a firmware template and assign the template to devices or device groups. In the firmware template, you can define what firmware version to install on FortiGate devices and all access devices, such as FortiAP, FortiSwitch, and FortiExtender. When you assign the template to one or more devices or to a device group, a firmware upgrade job is scheduled to rectify the firmware version on all affected devices.

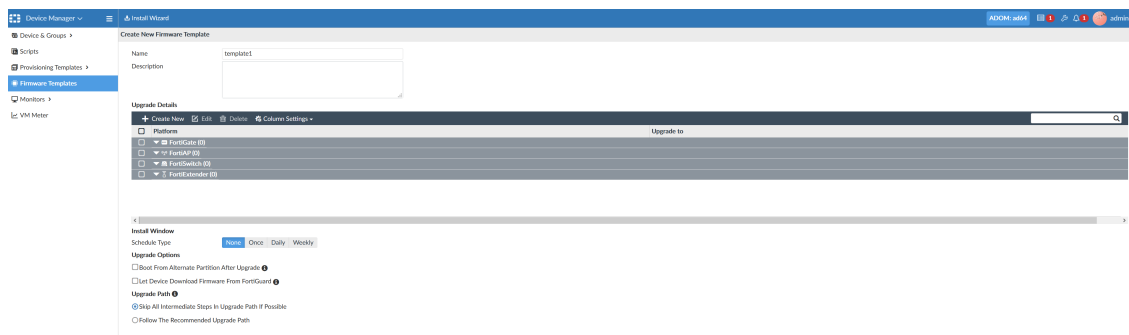
This topic contains the following sections:

- [Creating firmware upgrade templates for FortiGates on page 56](#)
- [Creating firmware templates for access devices on page 59](#)

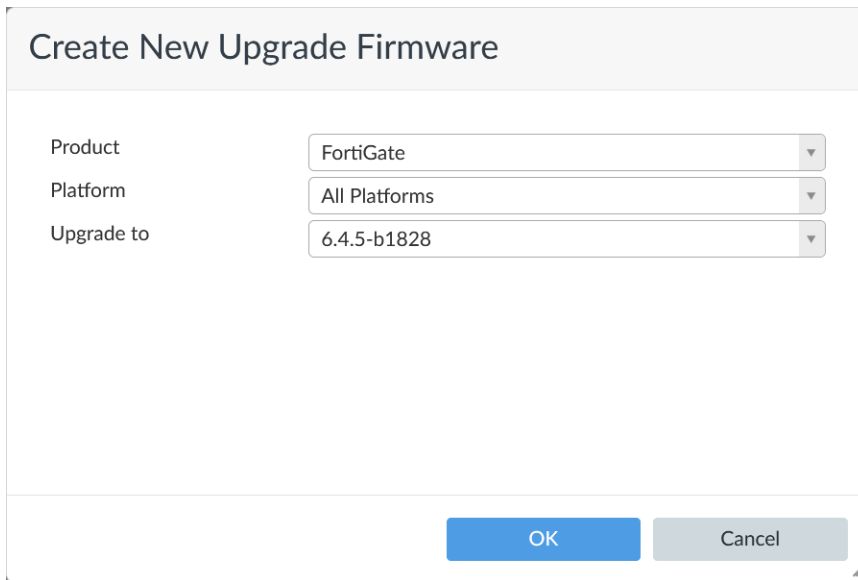
Creating firmware upgrade templates for FortiGates

To create a firmware template for FortiGates:

1. Go to *Device Manager > Device & Groups > Firmware Templates*, and click *Create New*. The *Create New Firmware Template* pane is displayed.



2. Create the FortiGate platform and specify the target FortiOS version:
 - a. Under *Upgrade Details*, click *Create New*. The *Create New Upgrade Firmware* dialog box is displayed.



Create New Upgrade Firmware

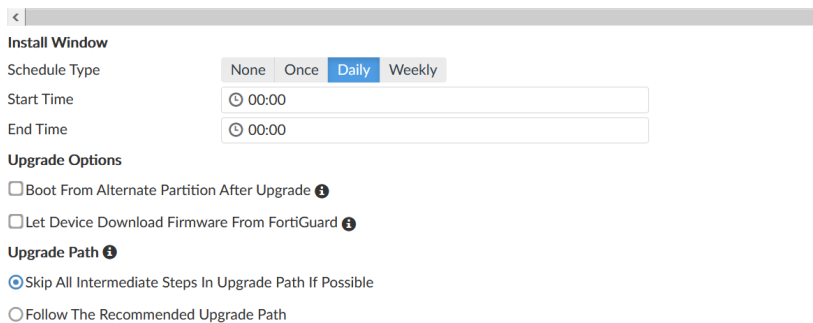
Product: FortiGate

Platform: All Platforms

Upgrade to: 6.4.5-b1828

OK Cancel

- b. In the *Product* list, select FortiGate.
 - c. In the *Platform* list, select a platform, or select *All Platforms*.
 - d. In the *Upgrade to* list, select the FortiOS version.
 - e. Click OK.
3. Under *Install Window*, select *None*, *Once*, *Daily*, or *Weekly* to specify when to start the upgrade. For the *Daily* and *Weekly* options, the upgrade starts when the scheduled time arrives. If the upgrade fails or does not finish in one upgrade window, the upgrade ceases, and then starts again when the schedule time arrives again.
- Example of the *Daily* option:



< |

Install Window

Schedule Type: None Once **Daily** Weekly

Start Time: 00:00

End Time: 00:00

Upgrade Options

☐ Boot From Alternate Partition After Upgrade ⓘ

☐ Let Device Download Firmware From FortiGuard ⓘ

Upgrade Path ⓘ

☒ Skip All Intermediate Steps In Upgrade Path If Possible

☐ Follow The Recommended Upgrade Path

Example of the *Weekly* option:

Install Window

Schedule Type: ☐ None ☐ Once ☐ Daily ☒ Weekly

Day: ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Start Time:

End Time:

Upgrade Options

☐ Boot From Alternate Partition After Upgrade ⓘ

☐ Let Device Download Firmware From FortiGuard ⓘ

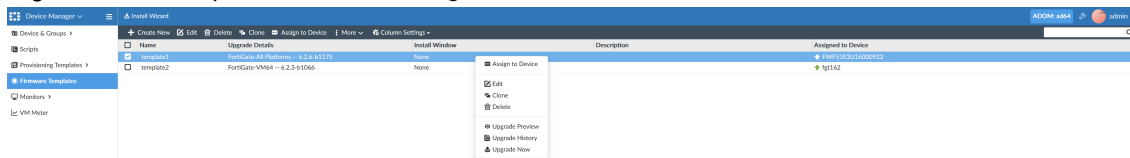
Upgrade Path ⓘ

☒ Skip All Intermediate Steps In Upgrade Path If Possible

☐ Follow The Recommended Upgrade Path

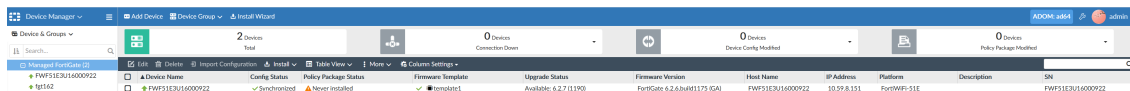
For example, create a firmware template with the *Daily* or *Weekly* option set to upgrade between 09:00 to 22:00, and assign the template to a device group with 98 devices at 21:45. FortiManager cannot finish upgrading all FortiGate devices in 15 minutes. As a result, the upgrade tasks fails for unfinished devices, but FortiManager resumes upgrading unfinished devices when the next scheduled upgrade window starts, which is 09:00 the next day.

4. Set the remaining options, and click **OK**.
The firmware template is created.
5. Assign the firmware template to one or more devices.
 - a. Right-click the template, and select **Assign to Device**.



The **Select Installation Targets** dialog box is displayed.

- b. In the **Available Entries** list, select one or more devices, and click **>** to move them to the **Selected Entries**.
- c. Click **OK**.



The template is assigned to the devices in the **Selected Entries** list. You can view the assigned devices on the **Device Manager > Device & Groups** pane.

6. Preview the upgrade and view the upgrade path.
 - a. Right-click the template, and select **Upgrade Preview**.
The **Firmware Upgrade Preview** dialog box is displayed. If there is an upgrade path, the path is displayed in the **Upgrade Path** column.

Firmware Upgrade Preview 'template2'

Device Name	Current Version	Upgrade To	Upgrade Path	Platform
FortiGate (1)				
fgt162	6.2.3-b1066	6.4.5-b1828	6.2.3-b1066->6.4.2-b1723->6.4.4-b1803->6.4.5-b1828	FortiGate-VM64

Close

b. Click *Close*.

7. After an upgrade completes, you can view upgrade history.

a. Right-click the template, and select *Upgrade History*.
The *Firmware Upgrade History* dialog box is displayed.

Firmware Upgrade History 'template1'

Upgrade Time: 2021-04-25 15:27:09 (Success: 1, Failed: 0)

Total: 1/1 (Success: 1, Failed: 0)

Device Name	Status	Upgrade Path
FortiGate (1)		
FWF51E3U16000922	Success	6.2.7-b1190->6.2.6-b1175

Close

b. Click *Close*.

Creating firmware templates for access devices

When access devices, such as FortiAP, FortiSwitch, and FortiExtender, are attached to a FortiGate, you can create a firmware template for the access devices, and assign the template to the FortiGate.

To create a firmware template for access devices:

1. Go to *Device Manager > Device & Groups > Firmware Templates*, and click *Create New*. The *Create New Firmware Template* pane is displayed.
2. Specify the firmware version for FortiSwitch, FortiAP, and FortiExtender, as well as the install window, and click *OK*.

Edit Firmware Template

Name: test

Description:

Upgrade Details

Platform	Upgrade to
FortiGate (0)	
FortiAP (1)	
FortiAP-24D	6.0.6-b0044
FortiSwitch (1)	
FortiSwitch-248D-FPOE	3.6.0-b0432
FortiExtender (1)	
FortiExtender-40D	4.1.5-b0191

Install Window

Schedule Type: None **Once** Daily Weekly

Start Time: 2021/05/12 00:00

End Time: 2021/05/13 00:00

Upgrade Options

☐ Boot From Alternate Partition After Upgrade

☐ Let Device Download Firmware From FortiGuard

Upgrade Path

☒ Skip All Intermediate Steps In Upgrade Path If Possible

☐ Follow The Recommended Upgrade Path

3. Assign the firmware template to the FortiGate.
 - a. Right-click the template, and select *Assign to Device*. The *Select Installation Targets* dialog box is displayed.
 - b. In the *Available Entries* list, select the FortiGate, and click > to move it to the *Selected Entries*.

Select Installation Targets

Use Shift key for multiple selections and double click for moving one item.

Available Entries (1)

- Managed FortiGate

Selected Entries (1)

- FortiGate-140E-POE
IP: 10.3.172.50, Platform: FortiGate-140E-POE

OK Cancel

- c. Click *OK*. The template is assigned to the FortiGate. When the install window for the upgrade arrives, the upgrade begins, and an upgrade task is created under *System Settings > Task Monitor*.

The screenshot shows the FortiManager interface with the 'Task Monitor' tab selected. A task titled 'Task 4719: firmware template 'test' upgrade' is in progress, showing a 50% completion bar. The task details table lists the following items:

#	Name	Time Used	Status
1	FortiGate-140E-POE(FAP24D3X16000296->6.0.6-b44)	7m 33s	Update done successfully
2	FortiGate-140E-POE(FX04DA5918008556->4.1.5-b191)	8m 39s	(0%)
3	FortiGate-140E-POE(S248DF3X17000116->3.6.0-b432)	8m 39s	(52%)

When all firmware upgrades for the task complete, the task displays **100%**.

The screenshot shows the same task 'Task 4719: firmware template 'test' upgrade' now at 100% completion. The task details table lists the following items:

#	Name	Time Used	Status
1	FortiGate-140E-POE(FAP24D3X16000296->6.0.6-b44)	7m 33s	Update done successfully
2	FortiGate-140E-POE(FX04DA5918008556->4.1.5-b191)	18m 54s	Update done successfully
3	FortiGate-140E-POE(S248DF3X17000116->3.6.0-b432)	14m 3s	Update done successfully

If any of the upgrades for the task fail, the entire upgrade task is stopped, and the upgrade failure is reported in the task.

The screenshot shows a task titled 'Task 4720: firmware template 'test' upgrade' which has failed, indicated by a red 100% completion bar. The task details table lists the following items:

#	Name	Time Used	Status
1	FortiGate-140E-POE(FAP24D3X16000296->6.0.5-b37)	10m 54s	Taskline not finished as task closed
2	FortiGate-140E-POE(S248DF3X17000116->3.6.0-b430)	10m 34s	Taskline not finished as task closed

Central Management

This section lists the new features added to FortiManager for central management:

- [FortiSwitch Manager on page 62](#)
- [Extender Manager on page 74](#)

FortiSwitch Manager

This section lists the new features added to FortiManager for FortiSwitch manager:

- [FortiSwitch Manager central management improvements on page 62](#)
- [FortiSwitch per-device management improvements on page 69](#)
- [Diagnostics and tools for device health monitoring and registration with FortiCloud 7.0.1 on page 73](#)

FortiSwitch Manager central management improvements

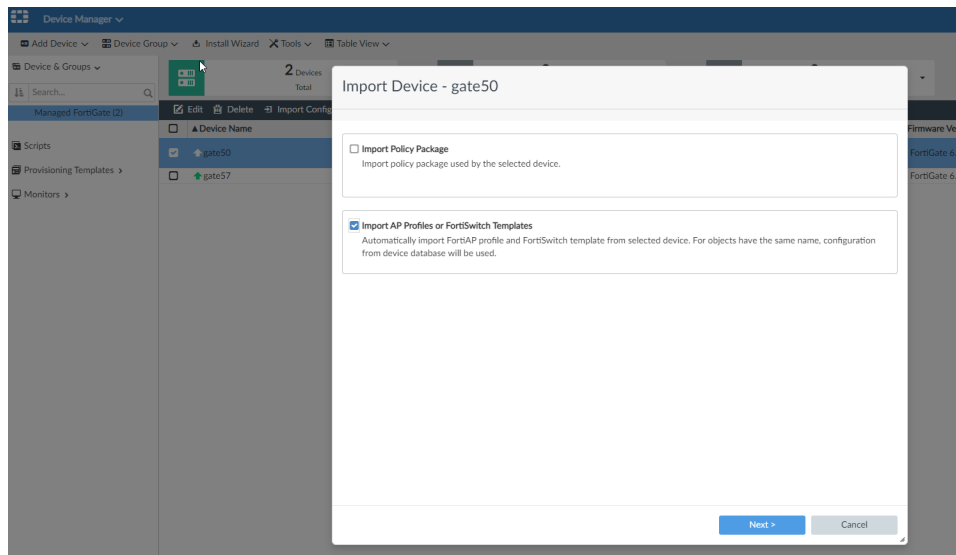
FortiSwitch Manager central management includes new improvements for MCLAG, QSFP split-port, switch custom commands and importing switch/AP configuration settings from FortiGate.

- [Importing FortiSwitch and FortiAP settings from FortiGate on page 62](#)
- [Split port configuration and display on page 64](#)
- [FortiSwitch custom commands in central management mode on page 67](#)
- [FortiSwitch custom commands in per-device management mode on page 68](#)

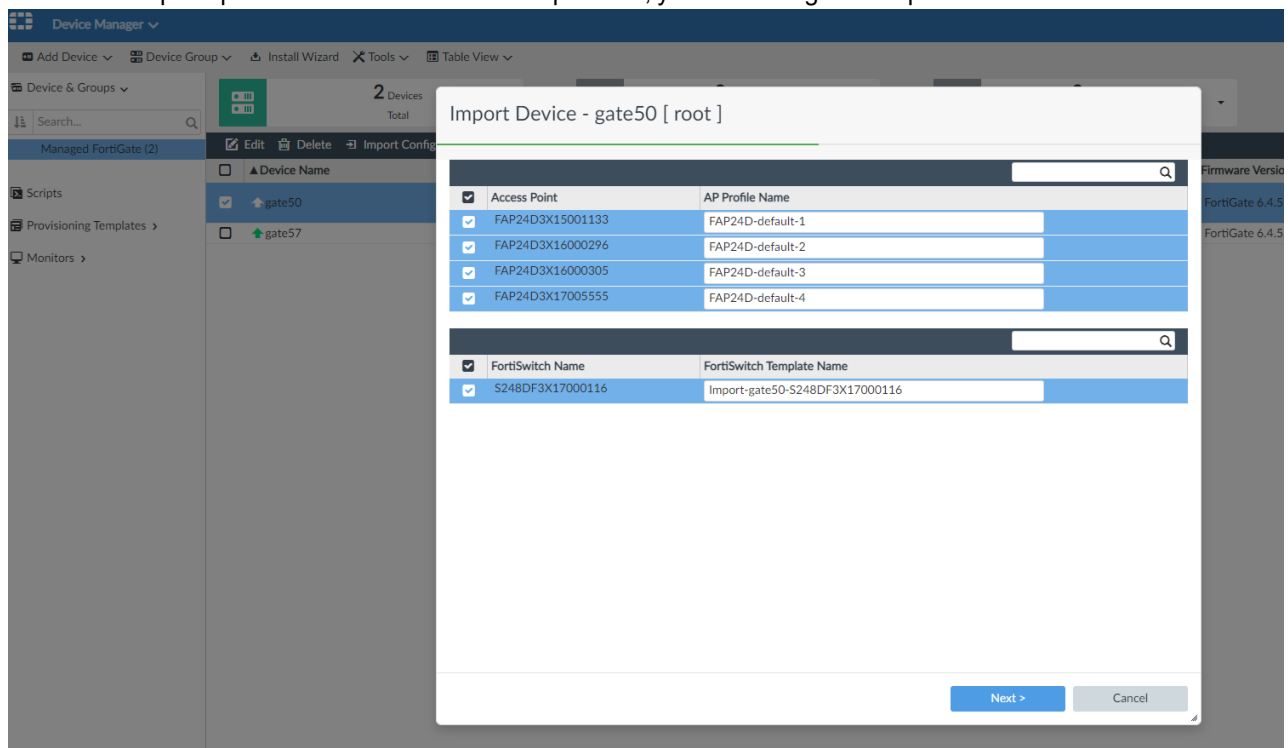
Importing FortiSwitch and FortiAP settings from FortiGate

To import FortiSwitch and FortiAP settings from FortiGate:

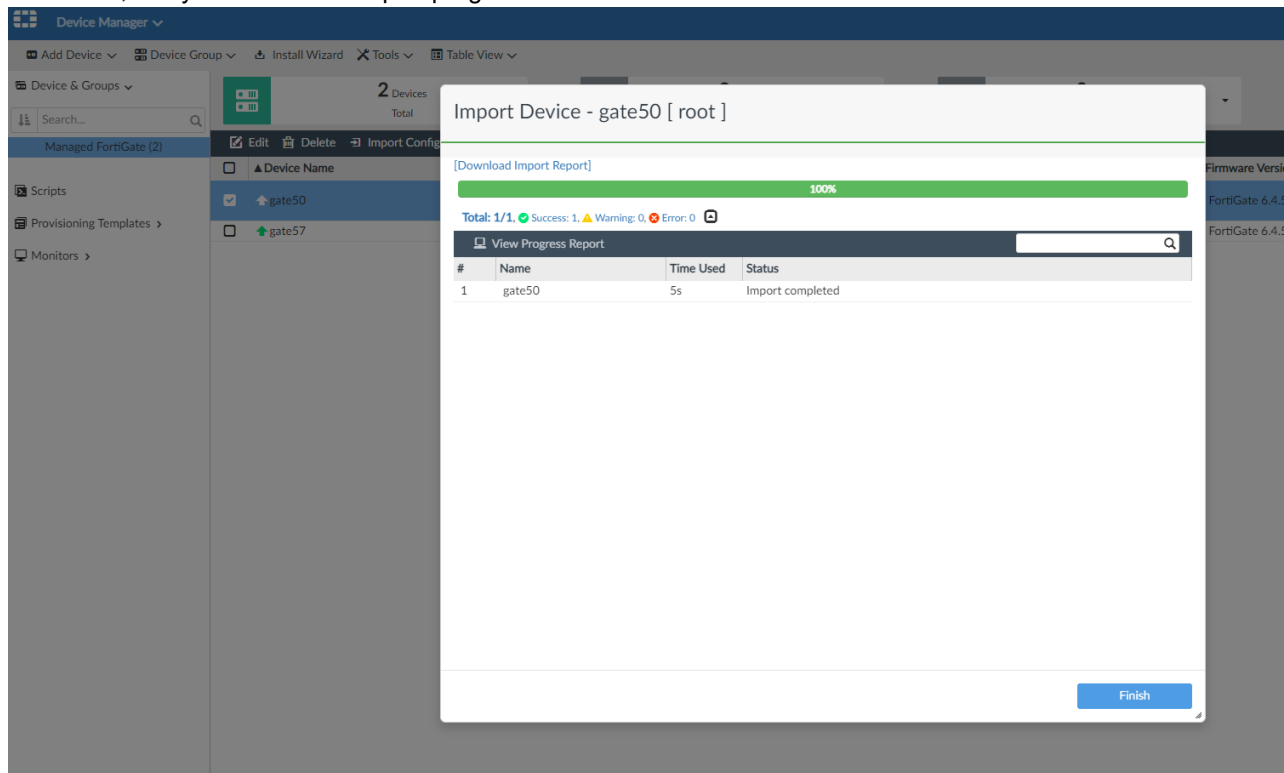
1. In *Device Manager*, right-click the FortiGate, click *Import Configuration*, then click *Import FortiAP Profiles and FortiSwitch Templates*.



2. In the access point profile list and FortiSwitch template list, you can change or keep the default name.



- 3.** Click *Next*, and you will see the import progress.



4. After the import is successful, go to **AP Manager > WiFi Templates > AP Profile**. The imported AP profiles are listed and they will be assigned to the managed APs directory.

+ Create New Edit Delete Clone Q Where Used Import Column Settings					
<input type="checkbox"/>	Name	Platform	Radio Mode	Bands	SSIDs
<input type="checkbox"/>	FAP24D-default	FAP24D	R1: Access Point	R1: 2.4GHz 802.11n/g	R1: All Tunnel Mode SSIDs
<input type="checkbox"/>	FAP24D-default-1	FAP24D	R1: Access Point	R1: 2.4GHz 802.11n/g	R1: All Tunnel Mode SSIDs
<input type="checkbox"/>	FAP24D-default-2	FAP24D	R1: Access Point	R1: 2.4GHz 802.11n/g	R1: All Tunnel Mode SSIDs
<input type="checkbox"/>	FAP24D-default-3	FAP24D	R1: Access Point	R1: 2.4GHz 802.11n/g	R1: All Tunnel Mode SSIDs
<input type="checkbox"/>	FAP24D-default-4	FAP24D	R1: Access Point	R1: 2.4GHz 802.11n/g	R1: All Tunnel Mode SSIDs

5. Go to *FortiSwitch Manager > FortiSwitch Templates > FortiSwitch Template*. The imported FortiSwitch templates are listed.

[illegible]

Split port configuration and display

To configure and view split ports:

1. Before adding the FortiSwitch to FortiGate, you must enable *phy-mode* on the FortiSwitch. Once the FortiSwitch has been authorized by FortiGate, you can add the FortiGate to FortiManager.

```

S548DN4K16000358 # conf switch phy-mode
S548DN4K16000358 (phy-mode) # show
config switch phy-mode
    set port-configuration disable-port54
    set port53-phy-mode 4x10G
end

```

2. In central management mode, import the template from the managed FortiSwitch, and the split port configuration will be retained.

You can edit the template including the split ports, and the changes can be installed to FortiGate when the template is assigned to the managed FortiSwitch.

Edit FortiSwitch Template

Template Name: 358
 Description: Imported from switch S548DN4K16000358
 Platforms: FortiSwitch-548D

Switch VLAN Assignments

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN
port48		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port49		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port50		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port51		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port52		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.1		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.2		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.3		Normal	Edge Port Spanning Tree Protocol	default	quarantine
port53.4		Normal	Edge Port Spanning Tree Protocol	default	quarantine

3. In the managed FortiSwitch, you can right-click on the FortiSwitch and click View Ports. The split ports are visible.

FortiSwitch Ports

MGMT

S548DN4K16000358

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE
port43		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port44		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port45		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port46		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port47		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port48		Normal	Edge Port Spanning Tree Protocol	FG200ETK18906777		
port49		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port50		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port51		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port52		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port53.1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port53.2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port53.3		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port53.4		Normal	Edge Port Spanning Tree Protocol	default	quarantine	

While mousing over the split ports, the port status is displayed.

FortiSwitch Ports

MGMT

S548DN4K16000358

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE
port1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port3		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port4		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port5		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port6		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port7		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port8		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port9		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port10		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port11		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port12		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port13		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port14		Normal	Edge Port Spanning Tree Protocol	default	quarantine	

Link Down

Native VLAN default

Allowed VLANs quarantine

STP Status Disabled

Port port53.2

FortiSwitch S548DN4K16000358

Link Down

Native VLAN default

Allowed VLANs quarantine

STP Status Disabled

Port port53.3

FortiSwitch S548DN4K16000358

Link Down

Native VLAN default

Allowed VLANs quarantine

STP Status Disabled

Port port53.4

FortiSwitch S548DN4K16000358

Link Down

Native VLAN default

Allowed VLANs quarantine

STP Status Disabled

Untrusted

4. In per-device management mode, users can edit split ports in the Port Configuration page.

FortiSwitch Ports

MGMT

S548DN4K16000358

+ Create New Edit Delete Column Settings

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	Device Information	DHCP Block
port43		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port44		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port45		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port46		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port47		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port48		Normal	Edge Port Spanning Tree Protocol	FG200ETK18906777				
port49		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port50		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port51		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port52		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port53.1		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port53.2		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port53.3		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted
port53.4		Normal	Edge Port Spanning Tree Protocol	default	quarantine			Untrusted

Edit

Delete

Status

Access Mode

POE

DHCP Blocking

IGMP Snooping

STP

Loop Guard

Edge Port

STP BPD Guard

STP Root Guard

While mousing over the split ports, the port status is displayed.

The screenshot shows the FortiSwitch Ports configuration page. At the top, there's a header with 'FortiSwitch Ports' and a 'MGMT' tab. Below the header is a table of ports. The table has columns: Port, Description, Access Mode, Enabled Features, Native VLAN, Allowed VLAN, and POE. The table lists ports from port43 to port53.4. Port53.1 is selected. A tooltip is displayed for port53.2, showing its status: Link Down, Native VLAN default, Allowed VLANs quarantine, STP Status Disabled, Port port53.2, FortiSwitch S548DN4K16000358, Link Down, Native VLAN default, Allowed VLANs quarantine, STP Status Disabled, Port port53.3, FortiSwitch S548DN4K16000358, Link Down, Native VLAN default, Allowed VLANs quarantine, STP Status Disabled, Port port53.4, FortiSwitch S548DN4K16000358, Link Down, Native VLAN default, Allowed VLANs quarantine, STP Status Disabled. The tooltip also shows 'Untrusted' status for port53.2, port53.3, and port53.4.

Port	Description	Access Mode	Enabled Features	Native VLAN	Allowed VLAN	POE
port43		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port44		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port45		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port46		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port47		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port48		Normal	Edge Port Spanning Tree Protocol	FG200ETK18906777	quarantine	
port49		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port50		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port51		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port52		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port53.1		Normal	Edge Port Spanning Tree Protocol	default	quarantine	
port53.2		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Untrusted
port53.3		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Untrusted
port53.4		Normal	Edge Port Spanning Tree Protocol	default	quarantine	Untrusted

FortiSwitch custom commands in central management mode

To configure custom commands in central management mode:

1. Go to *FortiSwitch Manager > FortiSwitch Templates > Custom Command*, and create a new custom command entry.

Edit Custom Command

Name: stp-age-10

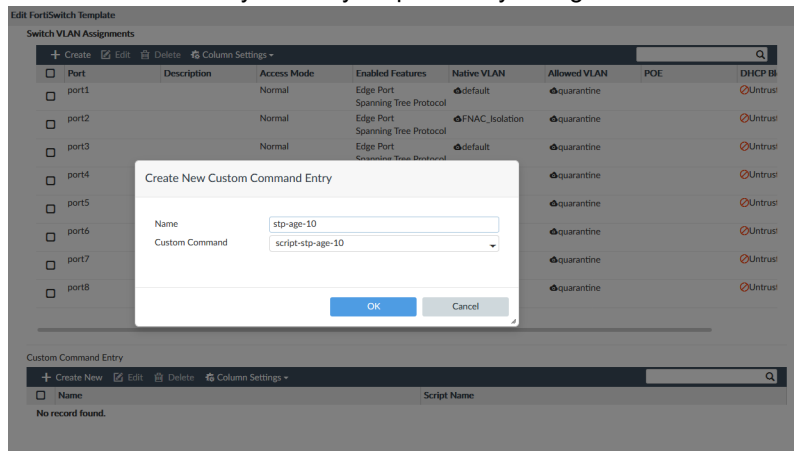
Description:

Command:

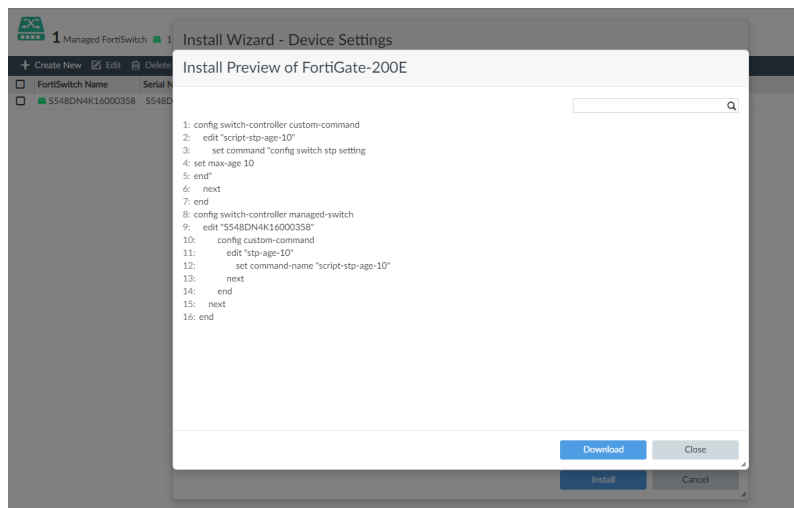
```
config switch stp setting
set max-age 10
end
```

44/4095

2. In *FortiSwitch Template*, edit or create a new template. Select *Create New* under *Custom Command Entry* to create a new command entry. Select your previously configured custom command, and click *OK*.



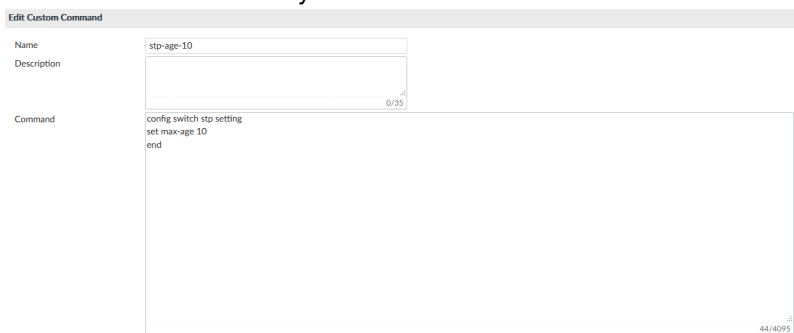
3. When the template is assigned to the FortiSwitch, the *Install Wizard* will install the custom command entry to FortiGate.



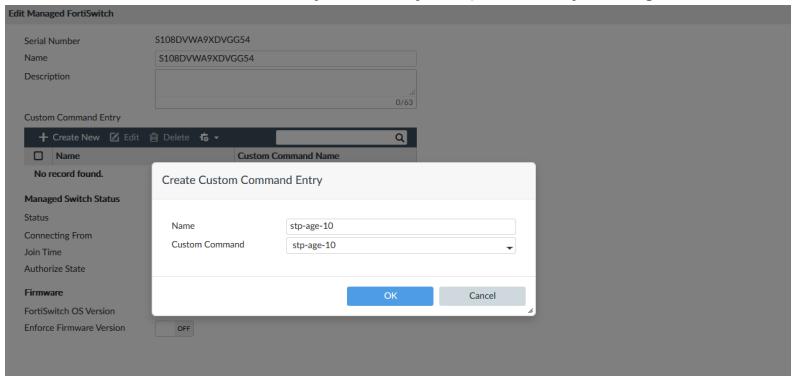
FortiSwitch custom commands in per-device management mode

To configure custom commands in per-device management mode:

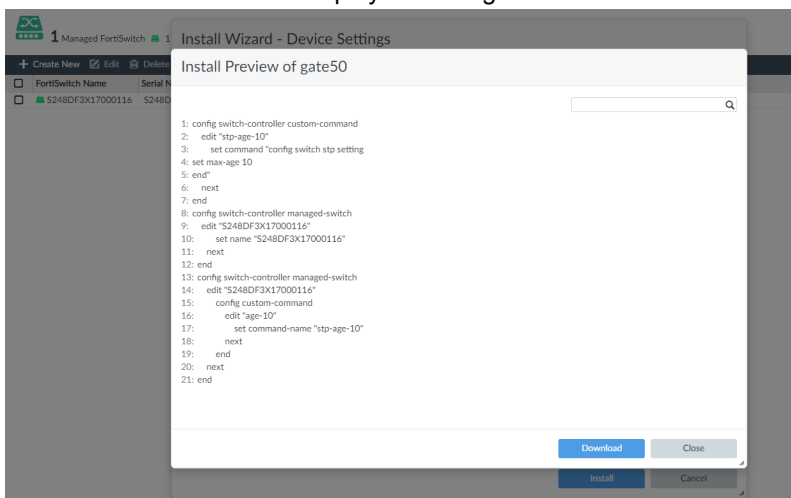
1. A custom command entry can be created/edited in *FortiSwitch Profiles > Custom Command* page for each FortiGate.



2. In *Managed Switches*, select and edit a FortiSwitch device, and in the custom command entry, select *Create New* to create a new command entry. Select your previously configured custom command, and click *OK*.



3. Use the *Install Wizard* to deploy the changes to FortiGate.



FortiSwitch per-device management improvements

FortiManager includes the following enhancements for FortiSwitch Manager when per-device management is enabled:

- NAC policy
- ports table
- connected device
- transceiver information

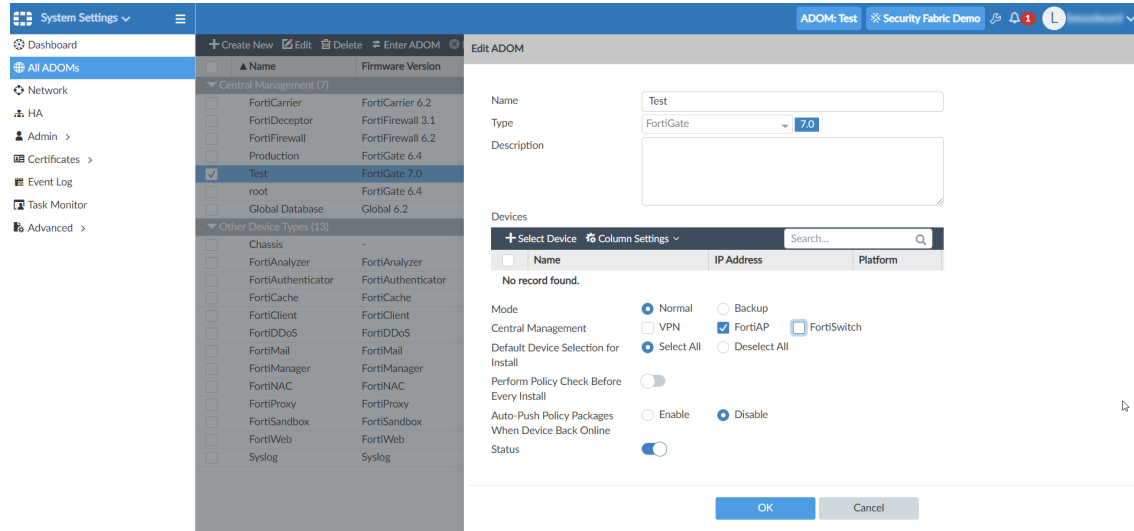


These features are only available in per-device FortiSwitch Management mode.

In addition, the *Policy & Objects* pane displays firewall object services in categories.

To enable FortiSwitch per-device management:

1. Go to *System Settings > All ADOMs*.
2. Double-click the ADOM to open it for editing.
3. Beside *Central Management*, clear the *FortiSwitch* checkbox, and click *OK*.



Central management is disabled, and per-device management is enabled for FortiSwitch.

NAC Policy

NAC policies can be created or edited in *FortiSwitch Profile > NAC Policies*. Once the policies are created or edited, the changes can be installed to the FortiGate.

To create NAC policies:

1. Go to *FortiSwitch Manager > FortiSwitch Profiles > NAC Policy*.
2. In the tree menu, select a FortiGate.
The NAC policies are displayed.
3. Click *Create New*.
The *Create New NAC Policies* pane opens.

Create New NAC Policies

Name:

Status: ☒ Enabled ☐ Disabled

Switch FortiLink:

FortiSwitches: 1 Entry Selected

Description:

Device Patterns:

- Category:
- MAC Address:
- Hardware Vendor:
- Device Family:
- Type:
- Operating System:
- User:
- Switch Controller Action:
- Assign VLAN:
- Bounce Port: ☒ ON

OK Cancel

- Complete the options, and click **OK**.
The changes are saved to the FortiGate database.

FortiSwitch Ports table GUI enhancements

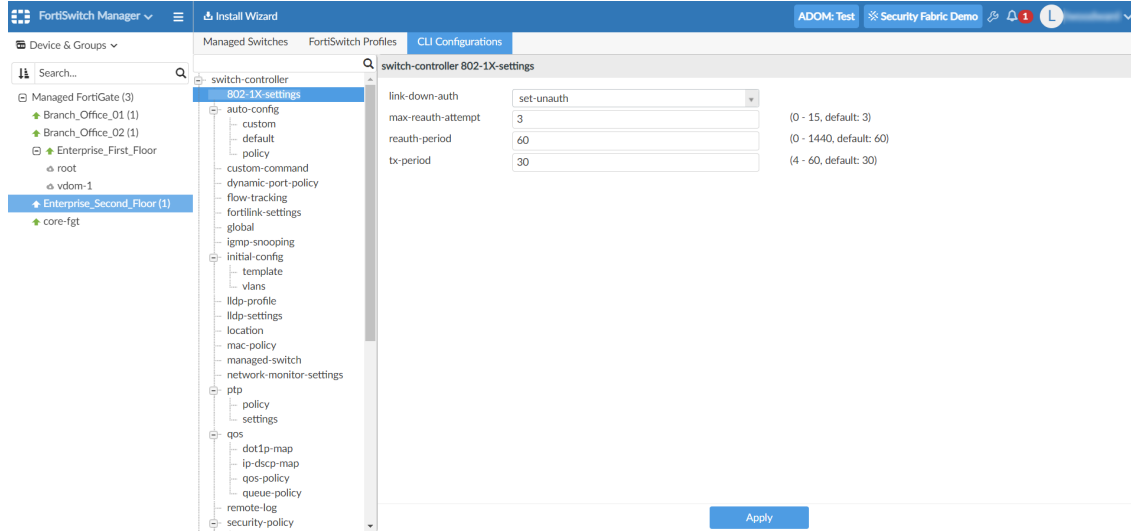
- Go to *FortiSwitch Manager > Managed Switches*.
- In the tree menu, select a FortiGate.
The list of managed switches is displayed in the content pane.
- Double-click a switch.
The *FortiSwitch Ports* pane opens.
The *Mode* column is added to show the port access mode.
The *Enabled Features* column is added to show if *Edge Port* or *Spanning Tree Protocol* is enabled.

Port	Description	Mode	Enabled Features	Native VLAN	Allowed VLAN	POE	Device Information	DHCP
port1		Static	Edge Port Spanning Tree Protocol	FGVM02TM210112E				
port2		Static	Edge Port Spanning Tree Protocol	vsw.port5	quarantine			Unit
port3		Static	Edge Port Spanning Tree Protocol	vsw.port5	quarantine			Unit
port4		Static	Edge Port Spanning Tree Protocol	vsw.port5	quarantine			Unit
port5		Static	Edge Port Spanning Tree Protocol	vsw.port5	quarantine			Unit
port6		Static	Edge Port Spanning Tree Protocol	vsw.port5	quarantine			Unit
port7		Static	Edge Port Spanning Tree Protocol	vsw.port5	quarantine			Unit
port8		Static	Edge Port Spanning Tree Protocol	vsw.port5	quarantine			Unit

The *Device Information* column is added to show the connected device information.
Hover over the listed device to see detailed information.
The *Transceiver* column is added to display transceiver information. If no transceiver is connected, then the *Transceiver* column shows *Unknown*.

FortiSwitch CLI Configuration

1. Go to *FortiSwitch Manager > CLI Configurations*.
2. In the tree menu, select a FortiGate.
The *CLI configurations* pane for the selected device is displayed.



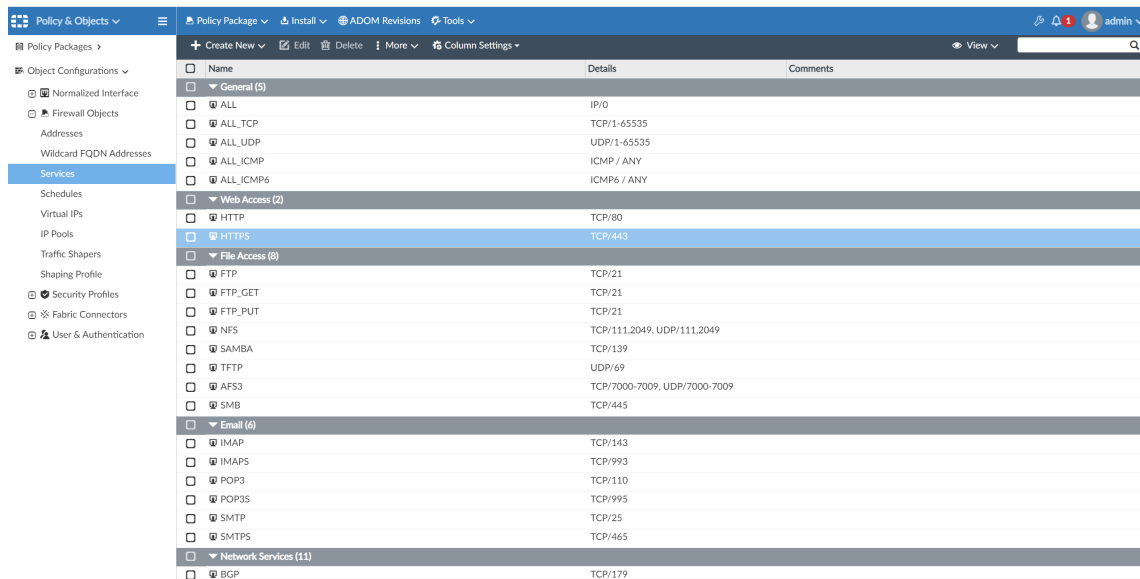
The *CLI Configurations* pane lets you view and edit all the settings for *switch-controller*.

Firewall object services

Firewall object services are now displayed in categories.

Firewall object services

1. Go to *Policy & Objects > Object Configurations > Firewall Objects > Services*.
The services are displayed in categories.

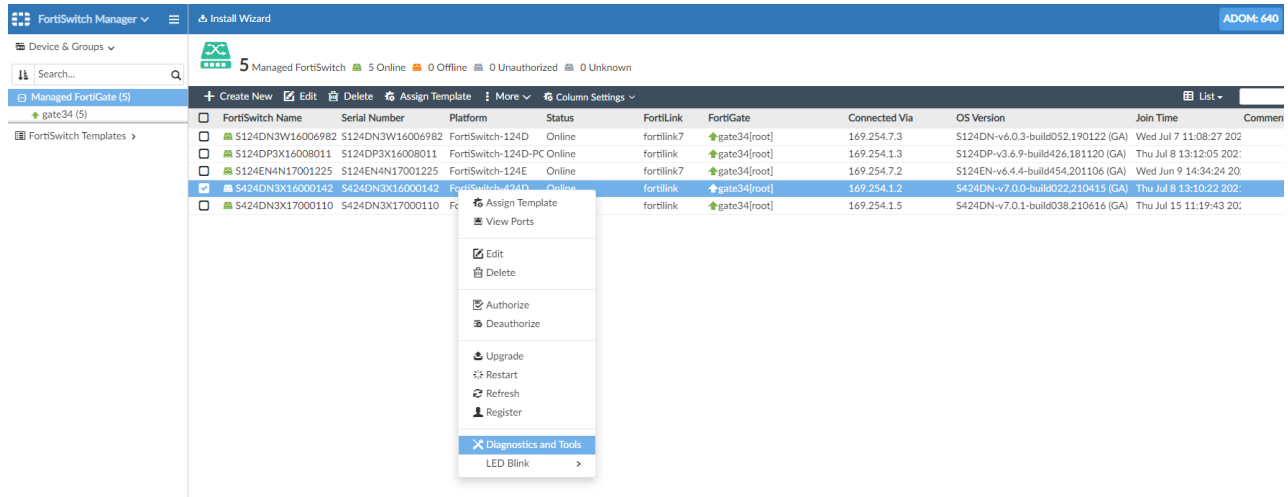


Diagnostics and tools for device health monitoring and registration with FortiCloud - 7.0.1

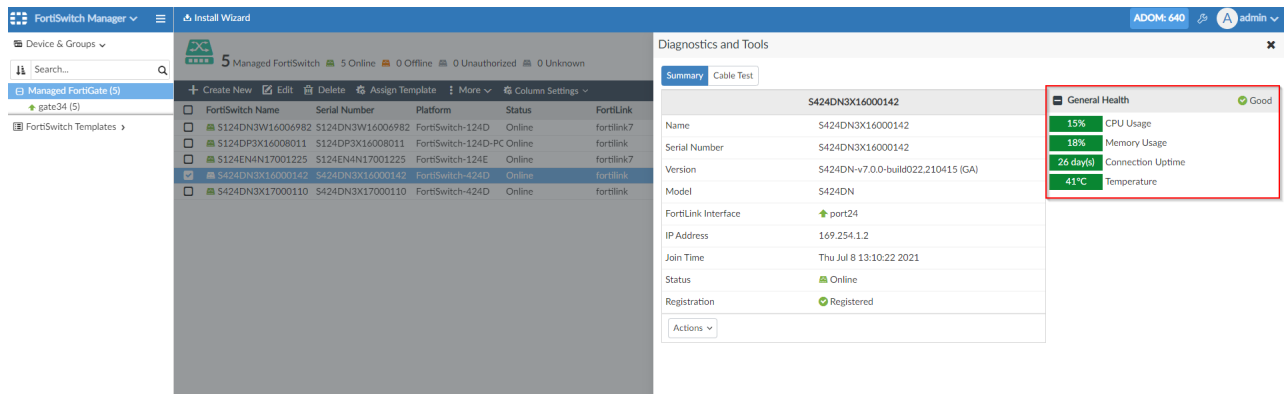
You can now see an overview of the general health for a managed FortiSwitch device. You can also register a device and view the registration status of a device.

To view general health and registration information:

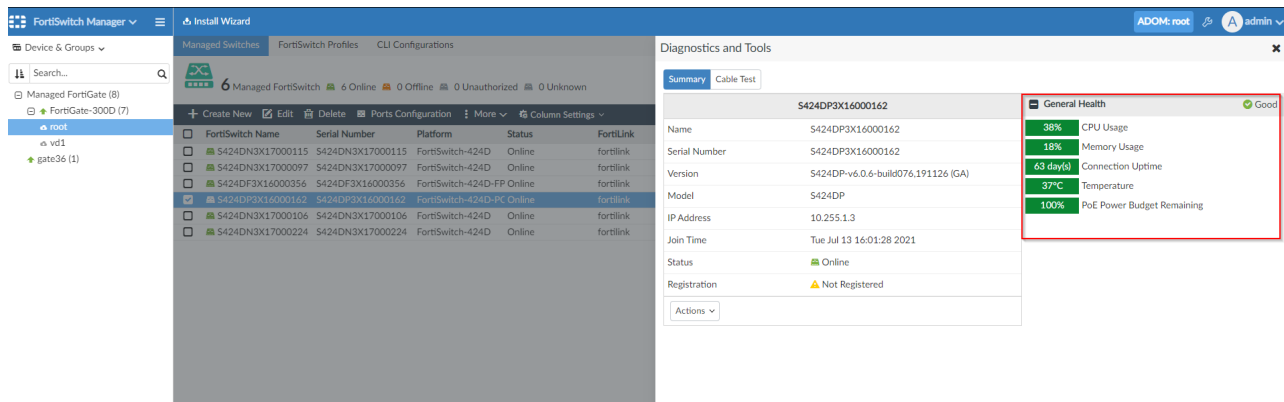
1. Go to *FortiSwitch Manager > Device & Groups*.
2. Right-click a managed device, and click *Diagnostics and Tools*.



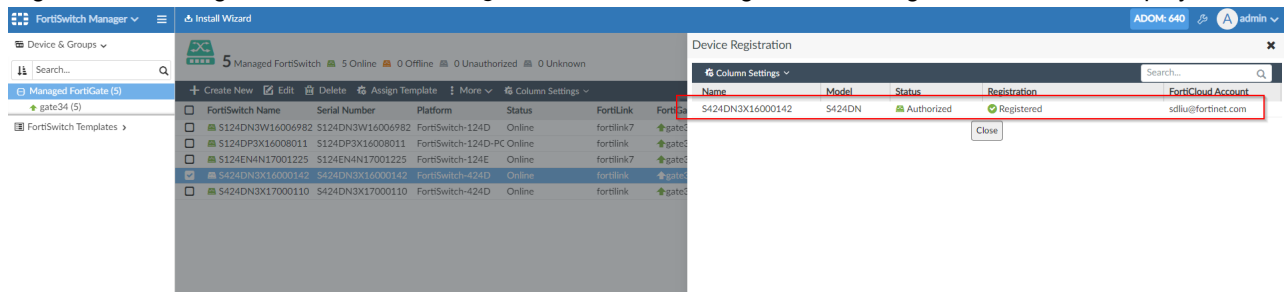
The *General Health* column displays the *CPU Usage*, *Memory Usage*, *Connection Uptime*, and *Temperature*.



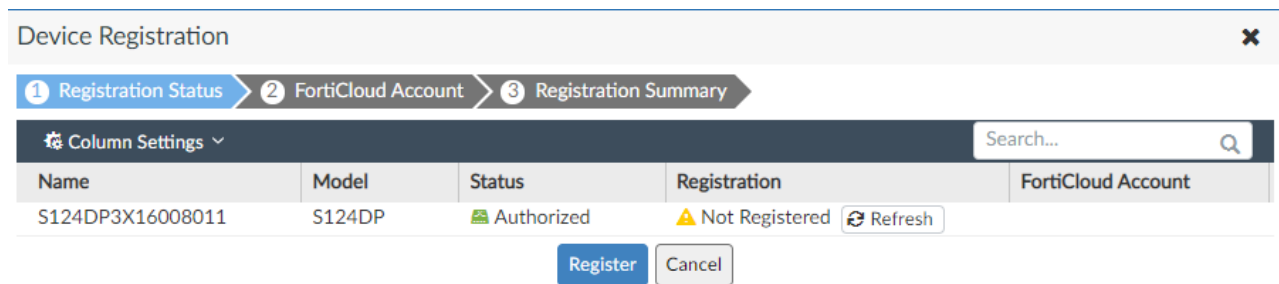
If the switch has PoE ports, the *PoE Power Budget Remaining* percentage is also displayed.



3. Right-click a managed device, and click *Register*. If the switch is registered, the registration status is displayed.



If the switch is not registered, click *Register* to register the switch with your FortiCloud Account.



Extender Manager

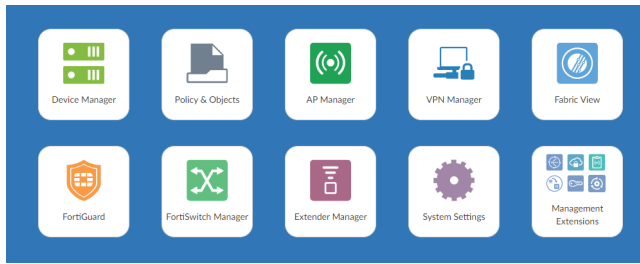
This section lists the new features added to FortiManager for Extender manager:

- Extender Manager for central managed FortiExtender devices on page 74
- FortiExtender Template for ZTP on page 78

Extender Manager for central managed FortiExtender devices

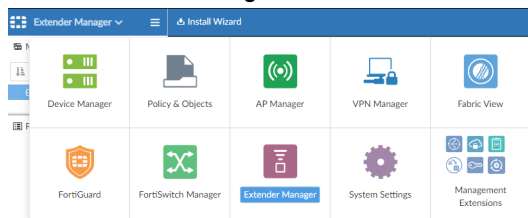
The Extender Manager allows you to create FortiExtender templates, SIM profiles, and Data plans. After a template is created, you can assign it to a managed device and install the profiles and plans on FortiExtender.

The FortiExtender module is always displayed in *Central Management* mode regardless of whether there is connection to a FortiExtender device.



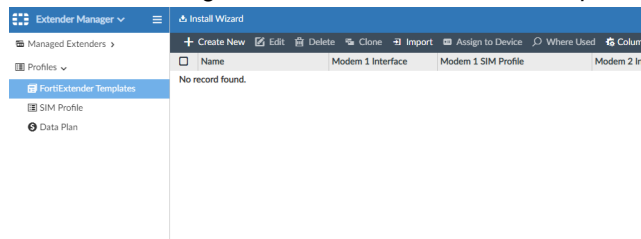
To create profiles with the Extender Manager:

1. Go to *Extender Manager*.

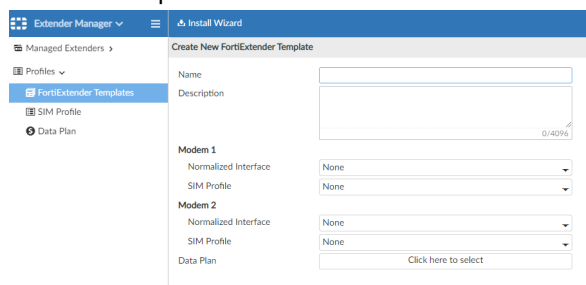


2. Create a FortiExtender template.

- a. In the tree menu, go to *Profiles > FortiExtender Templates*.

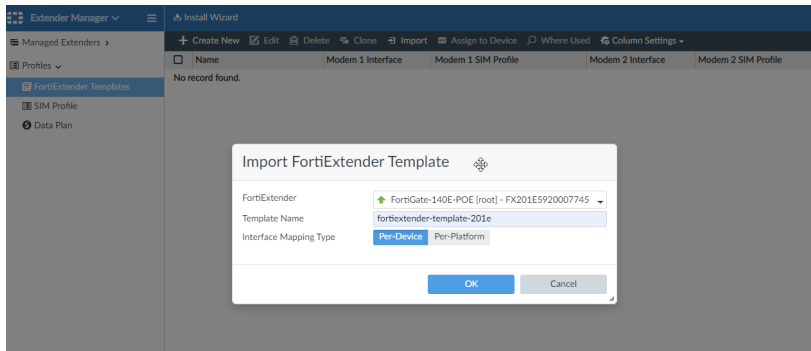


- b. In the toolbar, click *Create New*. The *Create New FortiExtender Template* page opens.
- c. Enter the template *Name* and click *OK*.

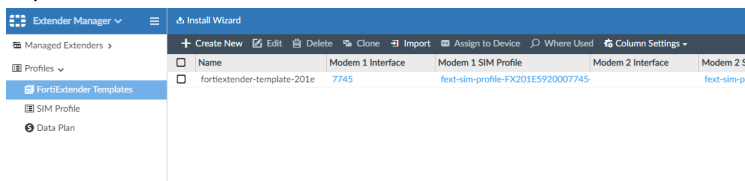


3. Import a FortiExtender template.

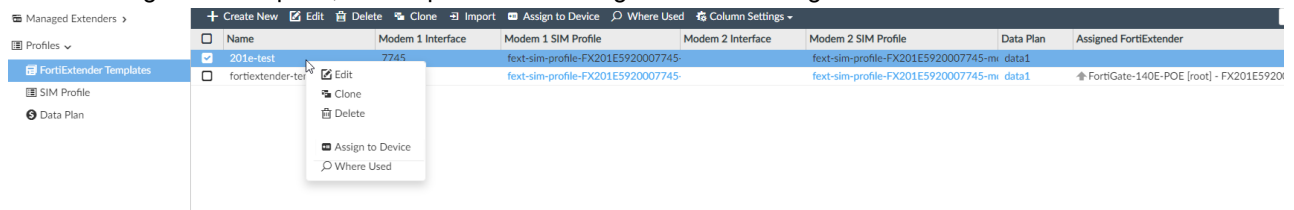
- In the toolbar, click **Import**. The *Import FortiExtender Template* dialog opens.
- Configure the template settings and click **OK**.



After importing the template, the template will be assigned to the FortiExtender where the template was imported from.



4. After creating a new template, the template can be assigned to an existing FortiExtender.



5. Create a SIM profile.

- In the tree menu, go to *Profiles > SIM Profile*.
- In the toolbar click **Create New**. The *Create New SIN Profile* dialog opens.

- c. Configure the profile settings and click OK.

Extender Manager ▾ **Install Wizard**

Managed Extenders ▸

Profiles ▾

FortiExtender Templates

SIM Profile

Data Plan

Create New SIM Profile

Name:

Description:

Default SIM: **SIM1** SIM2 Carrier Lowest Cost

SIM1 PIN: OFF

SIM2 PIN: OFF

GPS: ☒ ON

Auto SIM switch: ☒ ON

By disconnecting: OFF

By signal: OFF

By data plan: OFF

Switch back: ☐ Time ☐ Timer

Advanced Options ▸

6. Create a Data Plan profile.

- a. In the tree menu go to *Profiles* > *Data Plan*. The *Create New Data Plan* dialog opens.
- b. Configure the *Data Plan* profile settings and click OK.

Extender Manager ▾ **Install Wizard**

Managed Extenders ▸

Profiles ▾

FortiExtender Templates

SIM Profile

Data Plan

Create New Data Plan

Name:

Status: OFF

Available on: Modem 1 Modem 2 All Modems

Type: Carrier ATCA Slot ICCID Generic

Connectivity: ☒ None ☐ PAP ☐ CHAP

Authentication: ☒ IPv4 ☐ IPv6 ☐ IPv4 + IPv6

PDN Type:

Preferred Subnet:

APN:

Private Network: OFF

Billing Details: Monthly Data Limit: MB

Monthly Cost:

Billing Reset Day:

Overage: OFF

Smart Switch Threshold: Signal Threshold: -dBm

Signal Period: Seconds

Advanced Options ▸

7. Link the SIM profile and Data Plan profile to the FortiExtender template.

Edit FortiExtender Template

Name: 201e-test

Description:

Modem 1: Normalized Interface: 7745

SIM Profile: text-sim-profile-FX201E5920007745-modem1

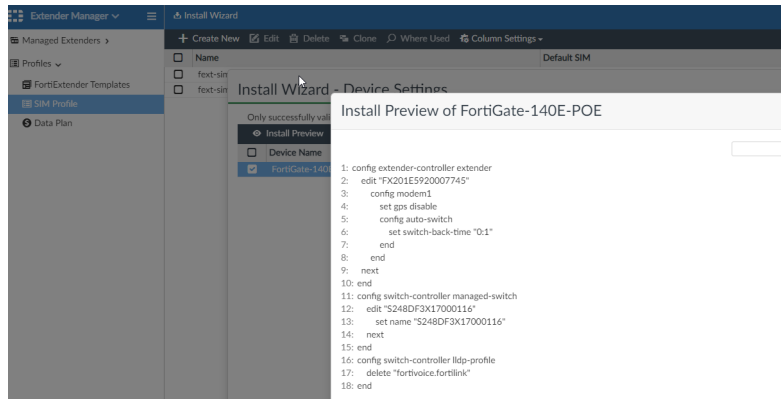
Modem 2: Normalized Interface: None

SIM Profile: text-sim-profile-FX201E5920007745-modem2

Data Plan: data1

1 Entry Selected

- After the template is assigned to a FortiExtender, the changes to the SIM profiles and Data plans can be installed to the FortiGate and FortiExtender.

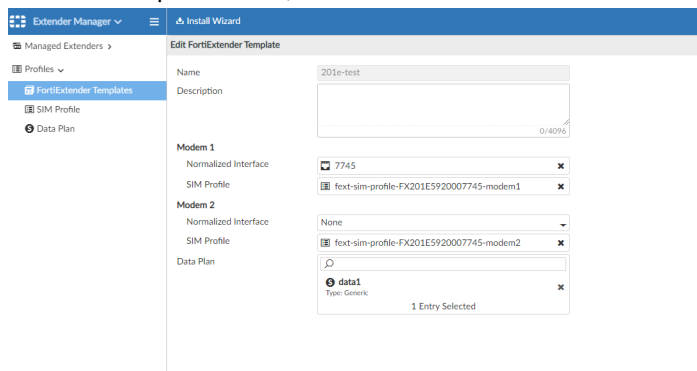


FortiExtender Template for ZTP

Use FortiExtender templates to configure SIM Profiles and Data Plans. After the template is created, you can assign it to a managed device.

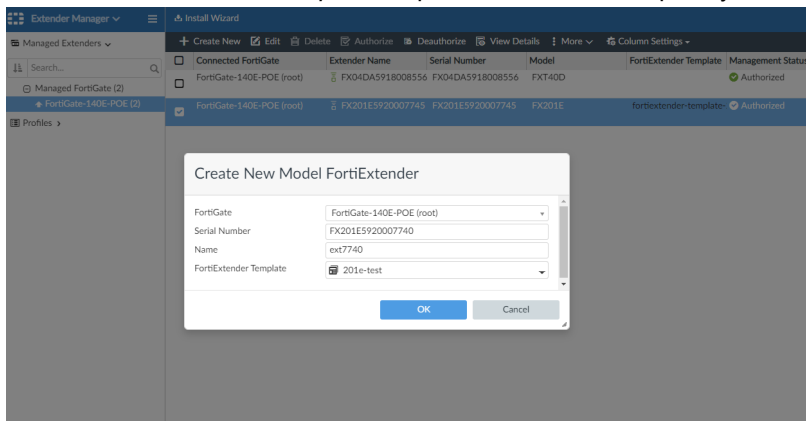
To create a FortiExtender template:

- Go to *Extender Manager > Profiles > FortiExtender Templates*.
- In the toolbar, click *Create New*. The *Create New FortiExtender Template* page opens.
- Enter the template *Name*, and select a *SIM Profile* and *Data Plan* from the dropdown list.

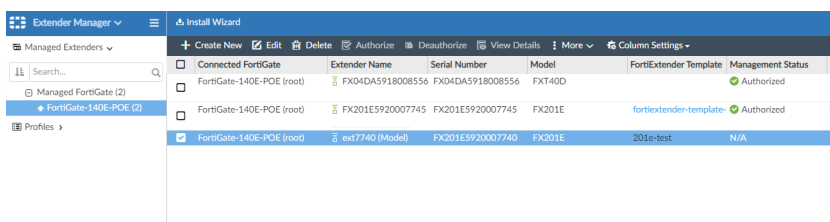


- Add the profile to a model FortiExtender.
 - Go to *Managed Extenders > Managed FortiGate(#)* and select a managed FortiGate.
 - In the toolbar, click *Create new*. The *Create New Model FortiExtender* dialog opens.

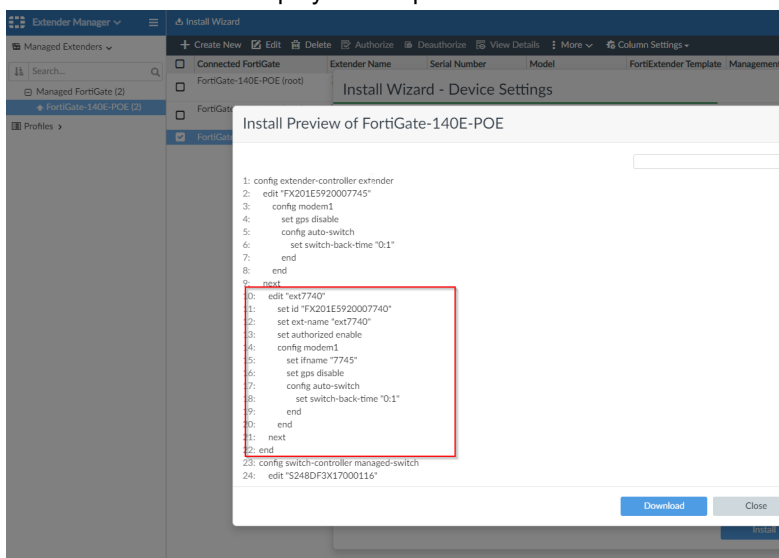
- c. From the *FortiExtender Template* dropdown, select the template you created and click OK.



The model device is added to the list.



5. Click *Install Wizard* to deploy the template to FortiGate.

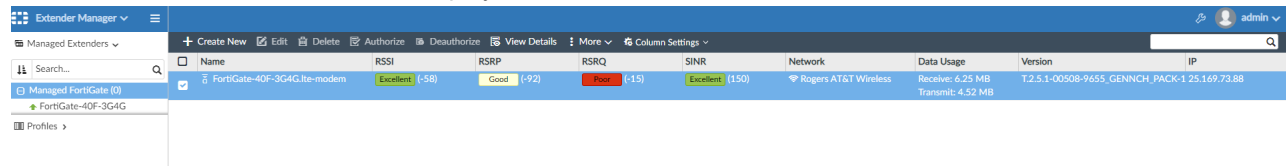


Retrieve and display RSSI information for FGT-xx-3G4G models - 7.0.1

The Extender Manager now displays the modem signal strength score and connection details for FortiGate 3G4G models. The LTE modems built into FortiGate 3G4G models will appear as managed devices in the tree menu.

To view FortiGate 3G4G modem details:

1. Go to *Extender Manager*.
2. In the tree menu, go to *Managed Extenders > Managed FortiGate*, and then select a 3G4G modem. The *RSSI*, *RSRP*, *RSRQ*, and *SINR* scores are displayed.



The screenshot shows the FortiManager Extender Manager interface. On the left, a tree menu is expanded to 'Managed FortiGate (0)', which contains a sub-item 'FortiGate-40F-3G4G'. The main area displays a table of modem details for 'FortiGate-40F-3G4G-ite-modem'. The table includes columns for Name, RSSI, RSRP, RSRQ, SINR, Network, Data Usage, Version, and IP. The RSSI, RSRP, and SINR columns show status indicators (Excellent, Good, Poor) and numerical values. The Network column shows 'Rogers AT&T Wireless'. The Data Usage column shows 'Receive: 6.25 MB' and 'Transmit: 4.52 MB'. The Version column shows 'T.2.5.1-00508-9655_GENNCH_PACK-1 25.169.73.88'.

Name	RSSI	RSRP	RSRQ	SINR	Network	Data Usage	Version	IP
FortiGate-40F-3G4G-ite-modem	Excellent (-50)	Good (-92)	Poor (-15)	Excellent (150)	Rogers AT&T Wireless	Receive: 6.25 MB Transmit: 4.52 MB	T.2.5.1-00508-9655_GENNCH_PACK-1	25.169.73.88

3. In the content pane, right-click the modem, and select *View Details*. The connection details are displayed.

Details of FortiGate-40F-3G4G.lte-modem

System Status

H/W Version	10001
S/W Version	T.2.5.1-00508-9655_GENNCH_PACK-1
Network Operator	Rogers AT&T Wireless
WAN Address	25.169.73.88
Default Gateway	25.169.73.89
Product	Sierra Wireless, Incorporated
Model	EM7565
Revision	SWI9X50C_01.08.04.00 dbb5d0 jenkins 2018/08/21 21:40:11
Manufacturer	Sierra Wireless, Incorporated
IMSI	302720398848981
RSSI	Excellent (-58)
LTE SINR	Excellent (150 dB)
LTE RSRQ	Poor (-15 dB)
LTE RSRP	Good (-92 dBm)
Connection Status	QMI_WDS_CONNECTION_STATUS_CONNECTED
ESN/MEID	
Activation	SIM_STATE_PRESENT
Roaming Status	false

Data Usage

Receive :6.25 MB
Transmit :4.52 MB

Close

Policy and Objects

This section lists the new features added to FortiManager for policy and objects:

- [Policy on page 82](#)
- [Objects on page 87](#)

Policy

This section lists the new features added to FortiManager for policies:

- [Policy revision history on page 82](#)
- [FortiGate 6000 and 7000 support for hit count 7.0.1 on page 87](#)
- [Assign multiple Global Policy Packages to the same ADOM, to different local Policy Packages 7.0.1 on page 85](#)

Policy revision history

You are now required to enter a change note when you create or edit a policy. Policy revisions can be viewed in the *Revision History* table.

To view the revision history:

1. Go to *Policy & Objects > Policy Packages*.
2. Double-click a policy in the list to edit it.
3. Revise the policy and then describe your edits in the *Change Note* field. You cannot save your changes until you enter a change note.

Edit Firewall Policy

Reverse Shaper: +

Per-IP Shaper: +

Logging Options

Log Traffic: ☐ No Log ☐ Log Security Events

☐ Capture Packets

☐ Generate Logs when Session Starts

Advanced

WCCP: ☐

Exempt from Captive Portal: ☐

Comments:

Advanced Options >

Revision

Change Note:

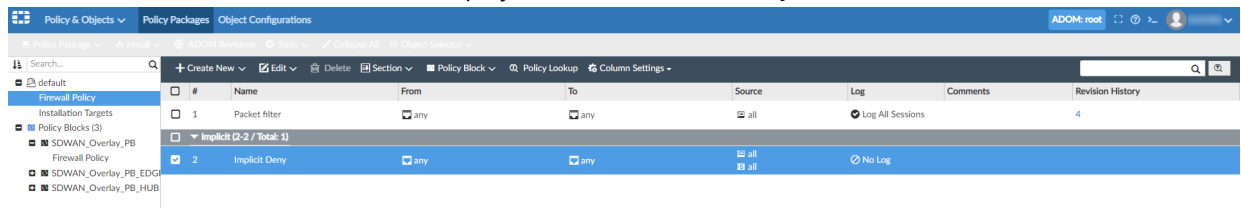
Change note is required

Revision History

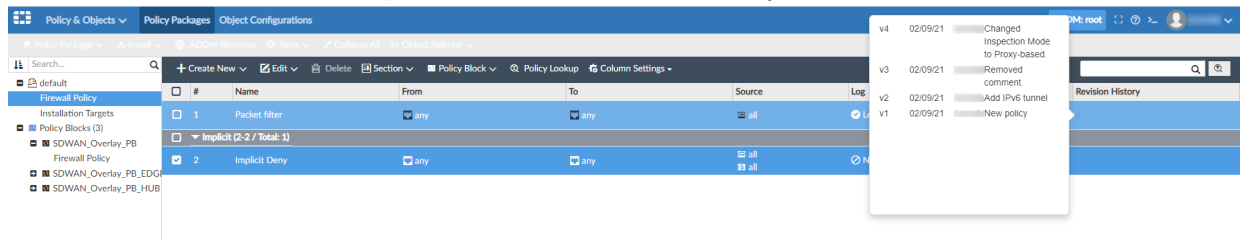
Revision	Changed by	Date/Time	Action	Change Note
4		2021-02-09 09:21:55	Modify	Changed Inspection Mode to Proxy-based.
3		2021-02-09 09:20:48	Modify	Removed comment.
2		2021-02-09 09:18:18	Modify	Add IPv6 tunnel
1		2021-02-09 09:17:02	Create	New policy

OK Cancel

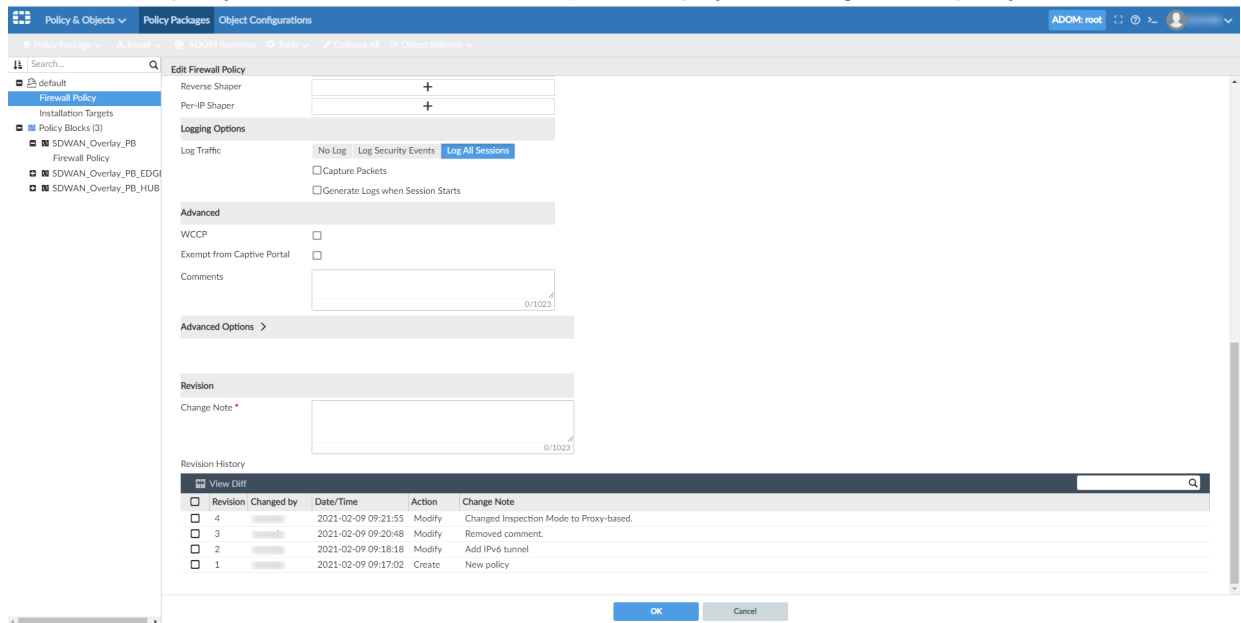
4. Click **OK**. The number of revisions are displayed in the *Revision History* column.



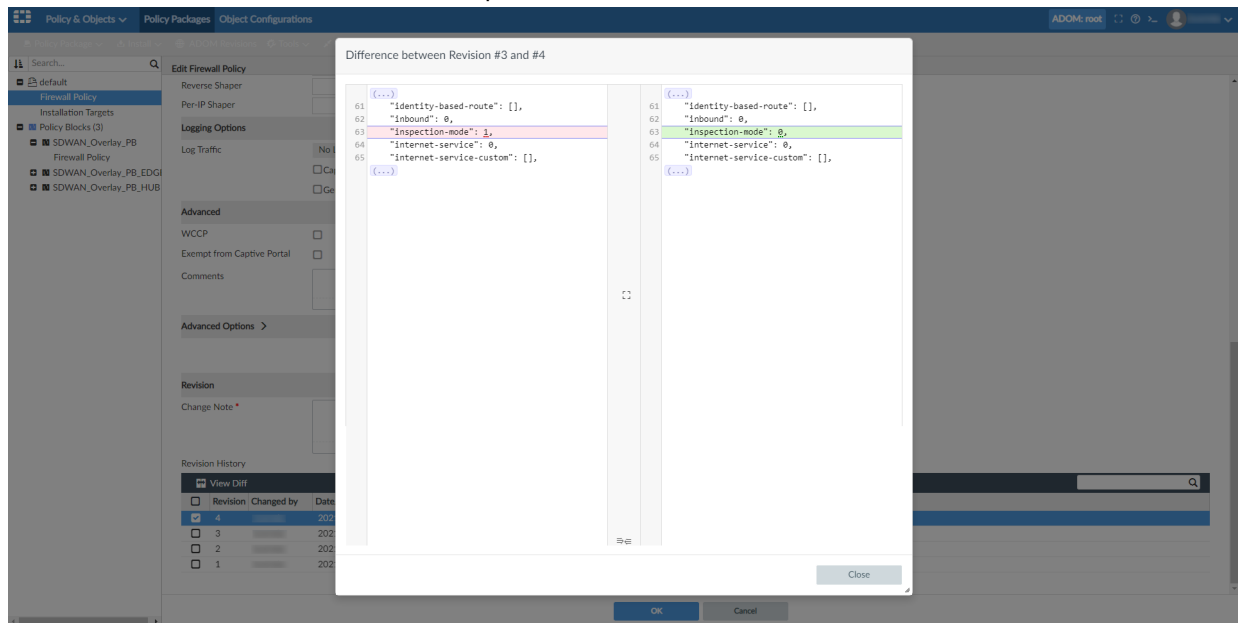
5. Click the link in the *Revision History* column to view the version history.



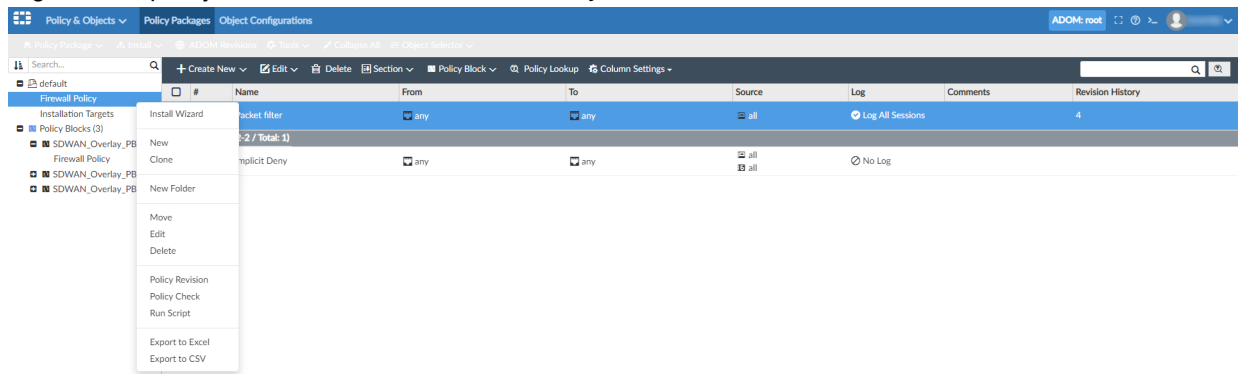
6. Double-click a policy in the list. The *Revision History* table displays the changes to the policy.



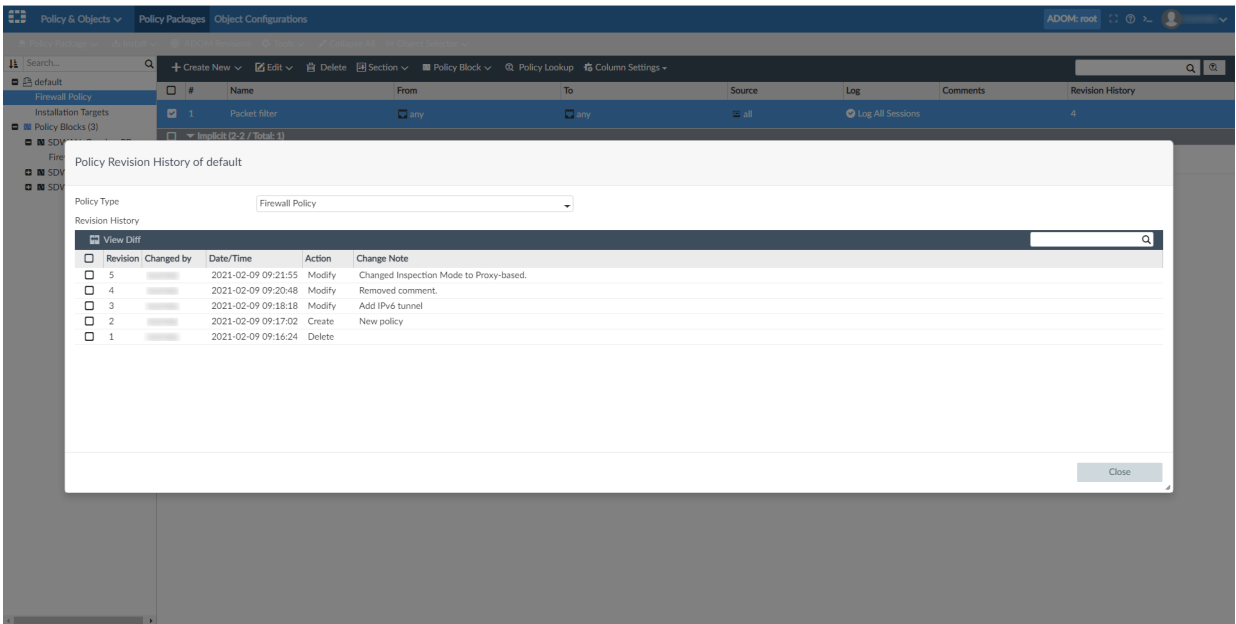
7. Select a revision, and click *View Diff* to compare versions.



8. Right-click a policy in the tree-menu, and select *Policy Revision*.



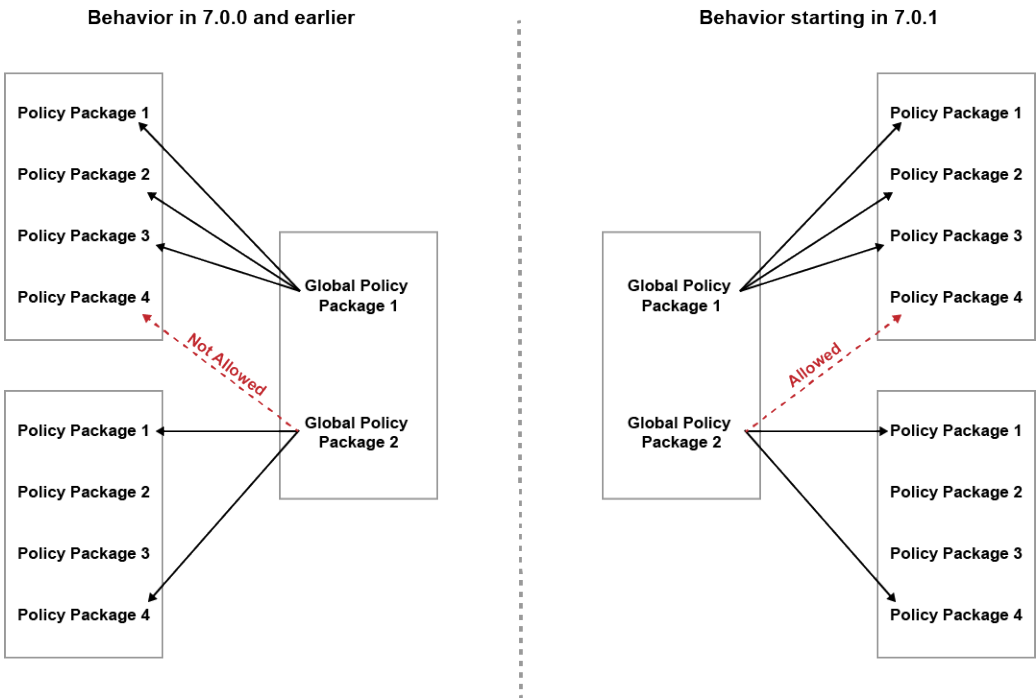
The Policy Revision history page is displayed.



Assign multiple Global Policy Packages to the same ADOM, to different local Policy Packages - 7.0.1

In FortiManager 7.0.1, you can now assign multiple Global Policy Packages to the same ADOM and to different local Policy Packages.

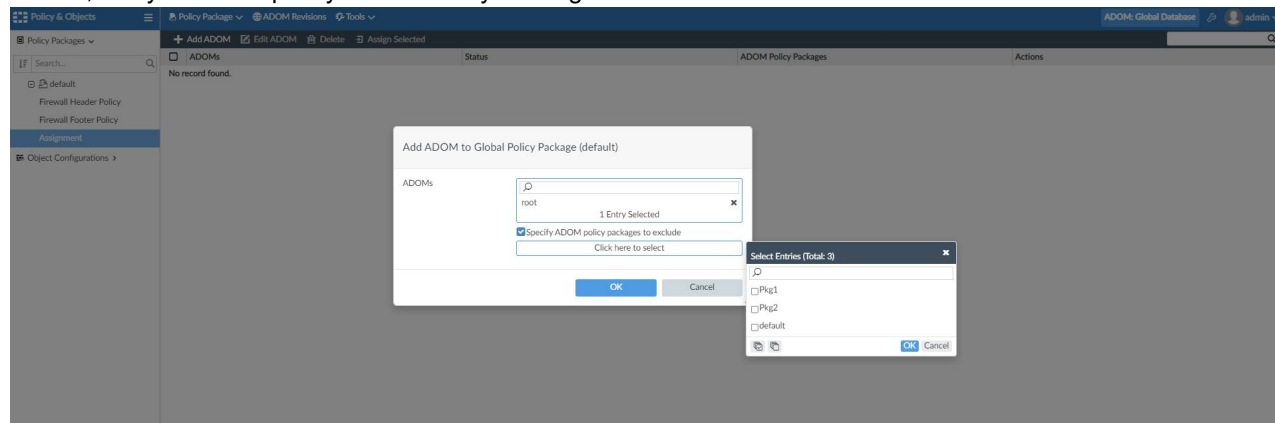
Topology



To assign global policy packages to local policy packages in an ADOM:

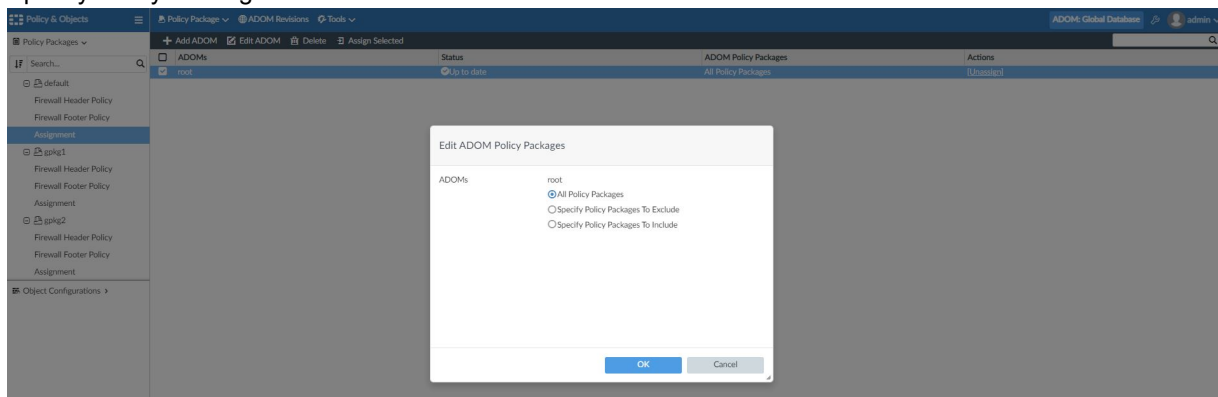
1. Enter the Global Database ADOM and go to *Policy & Objects > Policy Packages > select a policy package > Assignment*, and click *Add ADOM*.

Previously, Global Policy Package assignment included the ability to assign the Global Policy Package to a single ADOM, and you could specify ADOM Policy Packages to exclude.

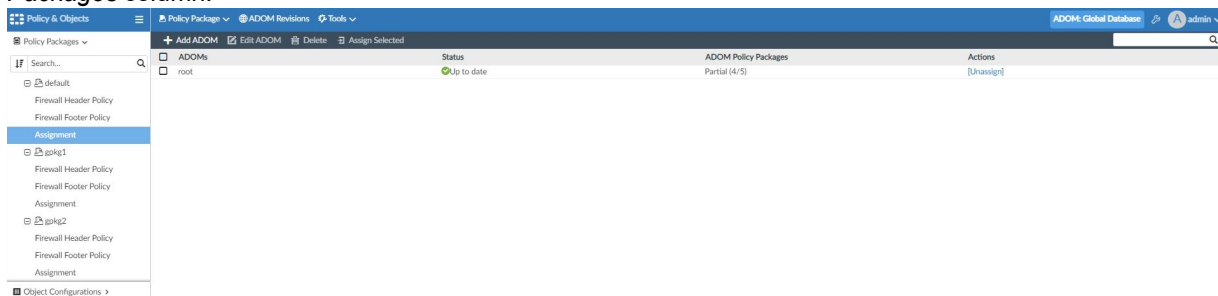


In 7.0.1, you now have additional options to install global policy packages to the policy packages in an ADOM:

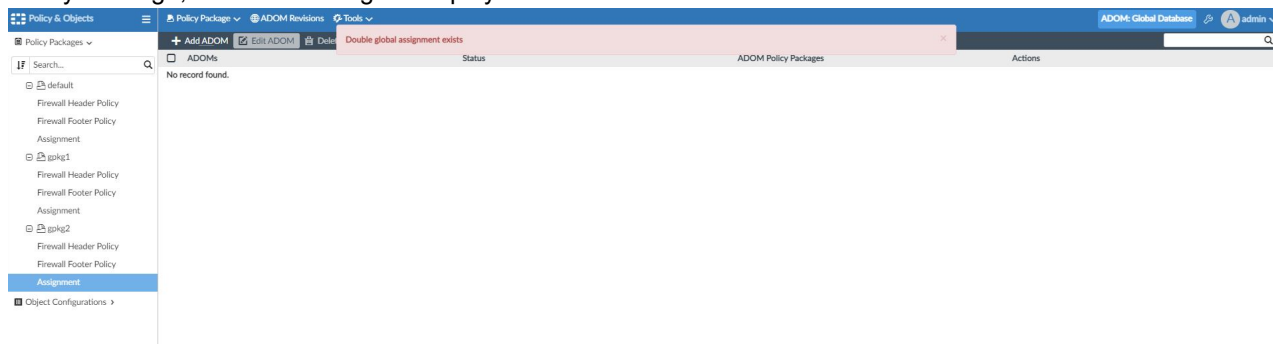
- All Policy Packages.
- Specify Policy Packages to Exclude.
- Specify Policy Packages to Include.



Go to *Policy & Objects > Policy Packages > select your policy package > Assignment*. Global Policy Packages assigned to a limited number of local Policy Packages in an ADOM are indicated as *Partial* in the *ADOM Policy Packages* column.



- When trying to add a new assignment to a local Policy Package which is already assigned by a different Global Policy Package, an error message is displayed.



FortiGate 6000 and 7000 support for hit count - 7.0.1

FortiGate 6000 and 7000 series models now support policy hit count queries in the GUI, similar to other FortiOS platforms.

To query policy hit counts on 6000 and 7000 series FortiGate devices:

- Go to *Policy Package*.
- Prior to FortiManager 7.0.1, FortiManager would display a hit count of 0 on the policy GUI page for 6000 and 7000 series FortiGate devices.

With this release, FortiManager can display hit count information in the GUI correctly.

#	From	To	Hit Count	Bytes	Packets	First Used	Last Used	Session Count	First Session	Last Session
1	p1-i2tp	vlan101	17	414.09 KB	4,483	2021/06/24 10:56	2021/06/24 11:16	1	2021/06/24 10:56	2021/06/24 11:09
2	p1-i2tp	vlan41	7	2.64 KB	44	2021/06/24 10:56	2021/06/24 11:40	0		
Implicit (3-3 / Total: 1)										
3	any	any	0	0.00 KB	0			0		

For example, the FortiGate 7060E's policy hit count is displayed.

ID	Name	From	To	Source	Destination	Schedule	Service	Security Profiles	Bytes	First Used	Hit Count	Last Used	Packets
1	vpn_i2tp_i2tp	p1-i2tp	vlan101	all	all	always	L2TP	no-inspection	412.99 kB	Hour ago	17	47 minutes ago	4,469
2		p1-i2tp	vlan41	all	all	always	ALL	no-inspection	2.64 kB	Hour ago	7	24 minutes ago	44
0	Implicit Deny	any	any	all	all	always	ALL		0 B		0		0

Objects

This section lists the new features added to FortiManager for objects:

- New IPS signatures monitoring page on page 88
- Object revision history on page 92

New IPS signatures monitoring page

The new IPS Signatures page allows you to quickly view and manage IPS signatures.

To display the IPS Signatures page:

1. Go to *Policy & Objects > Object Configurations*.
2. In the toolbar, click *Tools > Display Options*.
3. In the *Security Profiles* module, select *IPS Profiles*, and then click *OK*.

Admins can view the page by going to *Policy & Objects > Object Configurations > Security Profiles > IPS Signatures*.

ID	Name	Severity	Target	OS	Action	CVE-ID	Protocol
Custom IPS Signature (1)							
3102	Fun.Web.Products.Agent.Traffic				pass		
IPS Signature (13853)							
47306	10-Strike.LANState.Local.Buffer.Overflow.Exploit	medium	server,client	Windows	block		TCP,HTTP,FTP,SMTP
28273	2Wire.Wireless.Router.XSRF.Password.Reset	medium	server,client	Linux	block	CVE-2007-4387	TCP,HTTP
43545	3CX.Phone.System.VAD_Deploy.Arbitrary.File.Upload	high	server	Windows	block		TCP,HTTP
30316	3Com.3CDaemon.FTP.Server.Buffer.Overflow	high	server	Windows	block	CVE-2005-0277	TCP,FTP
10174	3Com.3CDaemon.FTP.Server.Information.Disclosure	low	client	Windows	block	CVE-2005-0278	TCP,FTP
26815	3Com.Intelligent.Management.Center.Information.Disclosure	medium	server	Windows	block		TCP,HTTP
27309	3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	medium	server	Linux	block		TCP,HTTP
48622	3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution	high	server	Linux	block		TCP,HTTP
32034	3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow	high	client	Windows	block		TCP,HTTP
40361	3S-Pocketnet.VMS.ActiveX.Control.Buffer.Overflow	medium	client	Windows	block	CVE-2014-9263	TCP,HTTP
48912	3S-Smart.CODESYS.CmpRouter.CmpRouterEmbedded.Integer.Overflow	high	server	Other	block	CVE-2019-5105	TCP
34892	3S-Smart.CODESYS.Gateway.Server.Directory.Traversal	high	server,client	Windows	block	CVE-2012-4705	TCP
35404	3S-Smart.CODESYS.Gateway.Server.DoS	high	server,client	Windows	block	CVE-2012-4707	TCP
41384	3S-Smart.CODESYS.Gateway.Server.Heap.Buffer.Overflow	high	server	Windows	block	CVE-2015-6460	TCP
30611	3S-Smart.CODESYS.Gateway.Server.Integer.Overflow	high	server	Windows	block	CVE-2011-5008	TCP
35280	3S-Smart.CODESYS.Gateway.Server.Memory.Access.Error	critical	server,client	Windows	block	CVE-2012-4704	TCP
35339	3S-Smart.CODESYS.Gateway.Server.OpCode.Heap.Buffer.Overflow	critical	server,client	Windows	block	CVE-2012-4706	TCP
35239	3S-Smart.CODESYS.Gateway.Server.Stack.Buffer.Overflow	critical	server,client	Windows	block	CVE-2012-4708	TCP
44031	3S-Smart.CODESYS.Web.Server.Buffer.Overflow	critical	server	Windows	block	CVE-2017-6025, CVE-2017-6026	TCP,HTTP
30528	3S-Smart.CODESYS.Web.Server.URI.Stack.Buffer.Overflow	high	server	Windows	block	CVE-2011-5007	TCP,HTTP
15186	3ivx.MPEG4.File.Processing.Buffer.Overflow	high	client	Windows	block	CVE-2007-6401	TCP,HTTP
17866	427BB.Cookie.Based.Authentication.Bypass	medium	server	Other	block	CVE-2006-0153	TCP,HTTP
17868	427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection	medium	server	Other	block	CVE-2006-0154	TCP,HTTP
30335	4D.WebStar.FTP.Command.Buffer.Overflow	high	server	Windows	block	CVE-2004-0695	TCP,FTP

Restricted Admin users can view the page by going to *Policy & Objects > Object Configurations > Intrusion Prevention > IPS Signatures*.

Restricted Admin Mode

ADOM: root

admin

Quick Install

Web Filter >

Intrusion Prevention >

Profiles

IPS Signatures

Application Control >

Create New

Edit

Delete

Column Settings

More

View Packages

View

ID	Name	Severity	Target	OS	Action	CVE-ID	Protocol
Custom IPS Signature (1)							
3102	Fun Web Products Agent Traffic				pass		
IPS Signature (13853)							
47206	10-Strike.LANState.Local.Buffer.Overflow.Exploit	medium	server,client	Windows	block		TCPIHTTP,FTP,SMTP,POP
28273	2Wire.Wireless.Router.XSRF.Password.Reset	medium	server,client	Linux	block	CVE-2007-4387	TCPIHTTP
43545	3CX.Phone.System.VAD_Deploy.Arbitrary.File.Upload	high	server	Windows	block		TCPIHTTP
30316	3Com.3CmDaemon.FTP.Server.Buffer.Overflow	high	server	Windows	block	CVE-2005-0277	TCPIFTP
10174	3Com.3CmDaemon.FTP.Server.Information.Disclosure	low	client	Windows	block	CVE-2005-0278	TCPIFTP
26815	3Com.Intelligent.Management.Center.Information.Disclosure	medium	server	Windows	block		TCPIHTTP
27309	3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	medium	server	Linux	block		TCPIHTTP
48622	3Com.OfficeConnect.Utility.CGML.Remote.Command.Execution	high	server	Linux	block		TCPIHTTP
32034	3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow	high	client	Windows	block		TCPIHTTP
40261	35-Pocketnet.VMS.ActiveX.Control.Buffer.Overflow	medium	client	Windows	block	CVE-2014-9263	TCPIHTTP
48912	35-Smart.CODESYS.CmpRouter.CmpRouterEmbedded.Integer.Overflow	high	server	Other	block	CVE-2019-5105	TCP
34892	35-Smart.CODESYS.Gateway.Server.Directory.Traversal	high	server,client	Windows	block	CVE-2012-4705	TCP
35404	35-Smart.CODESYS.Gateway.Server.DoS	high	server,client	Windows	block	CVE-2012-4707	TCP
41384	35-Smart.CODESYS.Gateway.Server.Heap.Buffer.Overflow	high	server	Windows	block	CVE-2015-6460	TCP
30611	35-Smart.CODESYS.Gateway.Server.Integer.Overflow	high	server	Windows	block	CVE-2011-5008	TCP
35280	35-Smart.CODESYS.Gateway.Server.Memory.Access.Error	critical	server,client	Windows	block	CVE-2012-4704	TCP
35339	35-Smart.CODESYS.Gateway.Server.Opcode Heap Buffer Overflow	critical	server,client	Windows	block	CVE-2012-4706	TCP
35239	35-Smart.CODESYS.Gateway.Server.Stack.Buffer.Overflow	critical	server,client	Windows	block	CVE-2012-4708	TCP
44031	35-Smart.CODESYS.Web.Server.Buffer.Overflow	critical	server	Windows	block	CVE-2017-6025, CVE-2017-60	TCPIHTTP
30528	35-Smart.CODESYS.Web.Server.URLLStack.Buffer.Overflow	high	server	Windows	block	CVE-2011-5007	TCPIHTTP
15186	3ivx.MPEG4.File.Processing.Buffer.Overflow	high	client	Windows	block	CVE-2007-6401	TCPIHTTP
17866	427BB.Cookie.Based.Authentication.Bypass	medium	server	Other	block	CVE-2006-0153	TCPIHTTP
17868	427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection	medium	server	Other	block	CVE-2006-0154	TCPIHTTP
30335	4D.WebStar.FTP.Command.Buffer.Overflow	high	server	Windows	block	CVE-2004-0695	TCPIFTP

To view and edit IPS signatures:

1. Go to *Policy & Objects > Object Configurations*.
2. Go to *Security Profiles > IPS Signatures*.
3. Click a predefined signature name. The *Information* page is displayed.

ADOM Revisions | Tools ▾

Create New

- ID 18149
- 41735
- 32583
- 45467
- 45977
- 45945
- 14870
- 12980
- 26516
- 13558
- 32027
- 17449
- 14014
- 32026
- 27599
- 29301
- 15157
- 14429
- 17838
- 25625
- 10572
- 27241
- 24219
- 34792
- 47800
- 12679
- 12442**

Information

Name
ASP.Data.FileAccess

Risk
Elevated

Summary
It indicates an attempt to access the source code of an Active Server Pages (ASP) page on a Microsoft Internet Information Service (IIS) server. There exists a vulnerability in IIS 3.0 and IIS 4.0 that allows the contents of the ASP file to be disclosed when the file name is appended, with "--\$DATA"; to the URL.

Signature Details

```
--service HTTP; --flow from_client; --pattern "asp"; --context uri; --no-case; --pattern "[3a3a]$DATA"; --context uri; --no-case; --distance 0;
```

Affected Products
Any unprotected IIS 3.0, 4.0 is vulnerable to the attack.

Action
Upgrade the IIS server to the latest non-vulnerable version or apply patch MS98-003.

Analysis
Attackers can obtain the source code of ASP files and may learn critical information about the victim system.

References

- <http://technet.microsoft.com/security/bulletin/MS98-003>
- <http://www.securityfocus.com/bid/149>
- CVE-1999-0278

Miscellaneous
ID 12442

Show Raw Data **Close**

Signs	View ▾	Protocol
block	CVE-ID LVE-2007-1297	TCP/HTTP
block		TCP/HTTP
block		TCP
block	CVE-2017-17932	TCP
block		TCP/HTTP
block	CVE-2018-6546	TCP/HTTP
pass	CVE-2007-3536	TCP/HTTP
block	CVE-2002-0307	TCP/HTTP
block		TCP/HTTP/NBSS
block	CVE-2006-5650	TCP/HTTP
block		TCP/HTTP
pass		TCP/HTTP
block	CVE-2005-1891	TCP/HTTP
block	CVE-2007-6699	TCP/HTTP
block		TCP/HTTP
block	CVE-2007-5755, CVE-2007-62	TCP/HTTP
pass	CVE-2006-5820	TCP/HTTP
pass	CVE-2009-3658	TCP/HTTP
pass	CVE-2007-6699	TCP/HTTP
pass	CVE-2001-0205	TCP/HTTP
block		TCP/HTTP
block		TCP/TFTPSM
block		TCP/HTTP
block		TCP/SSL
block	CVE-2002-0079	TCP/HTTP
block	CVE-1999-0278	TCP/HTTP

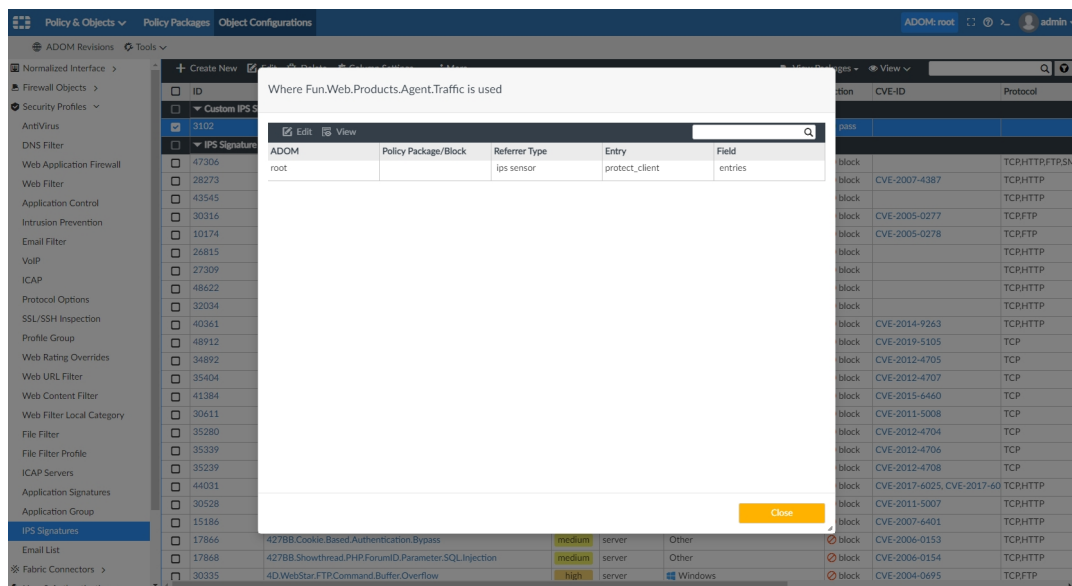
4. Click a predefined signature ID. The FortiGuard signature page opens in a new tab.

ID	Name	Severity	Target	OS	Action	CVE-ID	Protocol
18149	AJAXing.viewprofile.php:SQL-Injection	high	server	Windows, Linux, BSD, Solaris	block	CVE-2007-1297	HTTP
41735	AJQ.Botnet	critical	server	All	block		TCP/HTTP
32583	ALLMediaServer.Buffer.Overflow	high	server	Windows	block		TCP
45467	ALLPlayer.Group.ALLMediaServer.0.95.Buffer.Overflow	critical	server	Windows	block	CVE-2017-17932	TCP
45977	ALLPlayer.M3U.Overlong.URL.Buffer.Overflow	high	client	Windows	block		TCP/HTTP
45946	AMD.Gaming.Evolved.Raptor.Plays.TV.Service.Remote.File.Execution	critical	server	Windows	block	CVE-2018-6546	TCP/HTTP
148	AMX.VNC.ActiveX.Control.Access	high	client	Windows	pass	CVE-2007-3536	TCP/HTTP
12980	ANS.Directory.Traversal	high	server	Linux	block	CVE-2002-0307	TCP/HTTP
26516	AOL.Desktop.RTX.Buffer.Overflow	high	server,client	Windows	block		TCP/HTTP/NBSS
13558	AOL.ICQ.ActiveX.Control.Remote.Code.Execution	high	client	Windows	block	CVE-2006-5650	TCP/HTTP
32027	AOL.IWinAmp.ActiveX.Class.ConvertFile.Buffer.Overflow	high	client	Windows	block		TCP/HTTP
17449	AOL.IWinAmp.ActiveX.Class.ConvertFile.Method.Access	high	client	Windows	pass		TCP/HTTP
14014	AOL.Messenger.Buddy.Icon.DoS	low	client	Windows	block	CVE-2005-1891	TCP/HTTP
32026	AOL.Phobos.DLL.ActiveX.Control.Import.Buffer.Overflow	high	server,client	Windows	block		TCP/HTTP/FTP/SMTP
27599	AOL.Picture.Editor.YGPPicEdit.ActiveX.Control.Buffer.Overflow	low	client	Windows, Linux, MacOS	block	CVE-2007-6699	TCP/HTTP
29301	AOL.Picture.Editor.YGPPicEdit.DLL.ActiveX.Buffer.Overflow	high	client	Windows	block		TCP/HTTP
15157	AOL.Radio.ActiveX.Remote.Stack.Overflow	critical	client	Windows	block	CVE-2007-5755, CVE-2007-62	TCP/HTTP
14429	AOL.SuperBuddy.Link.SBIcons.ActiveX.Code.Execution	high	client	Windows	block	CVE-2006-5820	TCP/HTTP
17838	AOL.SuperBuddy.SetSuperBuddy.ActiveX.Control.Access	high	client	Windows	pass	CVE-2009-3658	TCP/HTTP
25625	AOL.YGPPicEdit.DLL.ActiveX.Control.Buffer.Overflow	high	client	Windows	pass	CVE-2007-6699	TCP/HTTP
10572	AOL.Server.Directory.Traversal	low	server	Windows	pass	CVE-2001-0205	TCP/HTTP
27241	APC.PowerChute.Network.Shutdown.HTTP.Response.Splitting	medium	server	All	block		TCP/HTTP
24219	APDF.WAV.To.MP3.Buffer.Overflow	high	server,client	Windows	block		TCP/FTP/NBSS/SMTP
34792	APT1.SSL.Certificate	medium	client	All	block		TCP/SSL
47800	APT34.Web.Shell	critical	client	Windows	block		TCP/HTTP
12679	ASP.Chunked.Transfer.Encoding	low	server	Windows	block	CVE-2002-0079	TCP/HTTP
12442	ASP.Data.File.Access	low	server	Windows	block	CVE-1999-0278	TCP/HTTP

5. Right-click the signature row. The context menu displays, *Edit*, *Clone* and *Delete* actions for custom signatures.

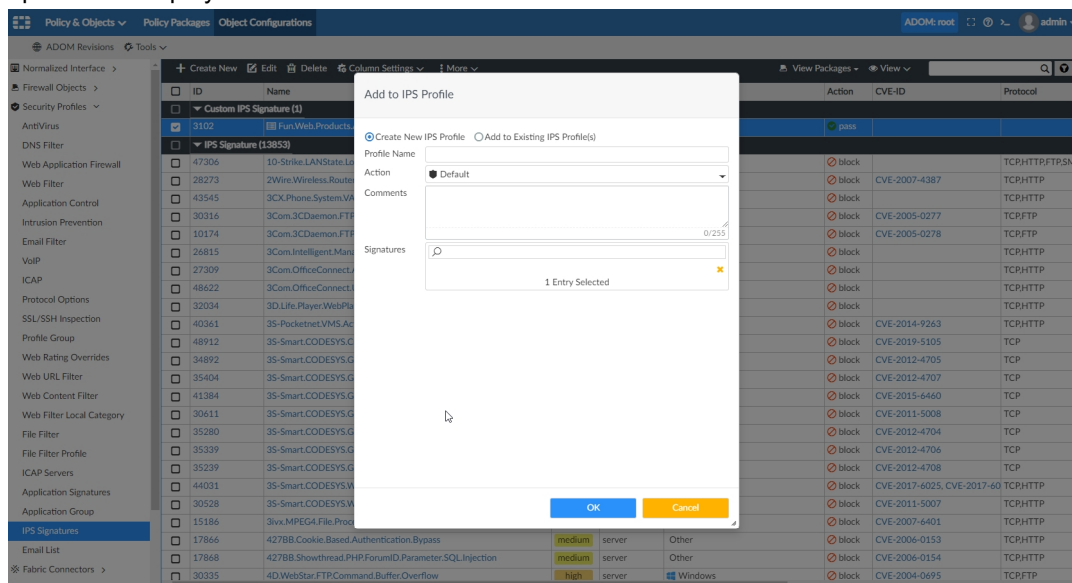
ID	Name	Severity	Target	OS	Action	CVE-ID	Protocol
3102	FunWeb.Products.Agent.Traffic	pass			pass		
47306	10-Strike.LANState.Local.Buffer.Overflow	medium	server,client	Windows	block		TCP/HTTP/FTP/SMTP
28273	2Wire.Wireless.Router.XSRF.Password.Reset	medium	server,client	Linux	block	CVE-2007-4387	TCP/HTTP
43545	3CX.Phone.System.VAD_Display.Arbitrary	high	server	Windows	block		TCP/HTTP
30316	3Com.3CDAemon.FTP.Server.Buffer.Overflow	high	server	Windows	block	CVE-2005-0277	TCP/FTP
10174	3Com.3CDAemon.FTP.Server.Information	low	client	Windows	block	CVE-2005-0278	TCP/FTP
26815	3Com.Intelligent.Management.Center.Information.Disclosure	medium	server	Windows	block		TCP/HTTP
27309	3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	medium	server	Linux	block		TCP/HTTP
48622	3Com.OfficeConnect.Utility.CG.Remote.Command.Execution	high	server	Linux	block		TCP/HTTP
32034	3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow	high	client	Windows	block		TCP/HTTP
40361	3S-Pocketnet.VMS.ActiveX.Control.Buffer.Overflow	medium	client	Windows	block	CVE-2014-9263	TCP/HTTP
48912	3S-Smart.CODESYS.CmpRouter.CmpRouter.Embedded.Integer.Overflow	high	server	Other	block	CVE-2019-5105	TCP
34892	3S-Smart.CODESYS.Gateway.Server.Directory.Traversal	high	server,client	Windows	block	CVE-2012-4705	TCP
35404	3S-Smart.CODESYS.Gateway.Server.DoS	high	server,client	Windows	block	CVE-2012-4707	TCP
41384	3S-Smart.CODESYS.Gateway.Server.Heap.Buffer.Overflow	high	server	Windows	block	CVE-2015-6440	TCP
30611	3S-Smart.CODESYS.Gateway.Server.Integer.Overflow	high	server	Windows	block	CVE-2011-5008	TCP
35280	3S-Smart.CODESYS.Gateway.Server.Memory.Access.Error	critical	server,client	Windows	block	CVE-2012-4704	TCP
35339	3S-Smart.CODESYS.Gateway.Server.OpCode.Heap.Buffer.Overflow	critical	server,client	Windows	block	CVE-2012-4706	TCP
35239	3S-Smart.CODESYS.Gateway.Server.Stack.Buffer.Overflow	critical	server,client	Windows	block	CVE-2012-4708	TCP
44031	3S-Smart.CODESYS.Web.Server.Buffer.Overflow	critical	server	Windows	block	CVE-2017-6025, CVE-2017-60	TCP/HTTP
30528	3S-Smart.CODESYS.Web.Server.URI.Stack.Buffer.Overflow	high	server	Windows	block	CVE-2011-5007	TCP/HTTP
15186	3ivx.MPEG4.File.Processing.Buffer.Overflow	high	client	Windows	block	CVE-2007-6401	TCP/HTTP
17866	427BB.Cookie.Based.Authentication.Bypass	medium	server	Other	block	CVE-2006-0153	TCP/HTTP
17868	427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection	medium	server	Other	block	CVE-2006-0154	TCP/HTTP
30335	4D.WebStar.FTP.Command.Buffer.Overflow	high	server	Windows	block	CVE-2004-0695	TCP/FTP

6. From the context menu, select *Where Used*. The *Where Used* dialog displays where the IPS profile signature is used. Clicking an IPS profile will open the IPS profile *Edit* window.



7. Click **Close**.

8. From the context menu, select **Add to IPS Profile**. the **Create New IPS Profile** and **Add to Existing IPS Profile(s)** options are displayed.



9. Click **Cancel**.

10. Type a search term in the in the **Search** field. The search results are highlighted in the signatures list.

The screenshot shows the 'Policy & Objects' interface with the 'Object Configurations' tab selected. The 'Search' field at the top right contains the text 'Remote'. The 'IPS Signatures' list is displayed, showing various signatures with their names, severities, targets, and actions. Signatures containing the word 'Remote' are highlighted in yellow.

ID	Name	Severity	Target	OS	Action	CVE-ID	Protocol
48622	3Com.OfficeConnect.Utility.Cgi.Remote.Command.Execution	high	server	Linux	block		TCP/HTTP
17732	4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow	medium	server	Windows	block	CVE-2005-1507	TCP/HTTP
26322	7-Technologies.IGSS.Opcode.Handling.Remote.Code.Execution	high	server	Windows	block	CVE-2011-1566	TCP
46263	7-Zip.RAR.Solid.Compression.Remote.Code.Execution	high	server/client	Windows	block	CVE-2018-10115	TCP/HTTP/TFTP/SMTP
47982	74CMS.Config.Controller.Remote.Code.Execution	critical	server	Windows, Linux, BSD, Solaris	block	CVE-2019-10684	TCP/HTTP
48617	ACTIA.SOC.Web.Configurator.Remote.Command.Execution	high	server	Other	block		TCP/HTTP
45945	AMD.Gaming.Evolved.Raptr.Plays.TV.Service.Remote.File.Execution	critical	server	Windows	block	CVE-2018-6546	TCP/HTTP
13558	AOL.ICQ.ActiveX.Control.Remote.Code.Execution	high	client	Windows	block	CVE-2006-5650	TCP/HTTP
15157	AOL.Radio.ActiveX.Remote.Stack.Overflow	critical	client	Windows	block	CVE-2007-5755, CVE-2007-62	TCP/HTTP
15651	ASUS.Remote.Console.Dppproxy.Buffer.Overflow	low	server	Windows	block	CVE-2008-1491	TCP
46543	ASUSTOR.ADM.script.Parameter.Remote.OS.Command.Execution	critical	server	Other, Linux	block	CVE-2018-11510	TCP/HTTP
30571	AVID.Photonic.Indower.Remote.Stack.Buffer.Overflow	high	server	Windows	block	CVE-2011-5003	TCP
12499	AWStats.Config.dir.Remote.Command.Execution	low	server	Windows, Linux	block	CVE-2005-0116	TCP/HTTP
26017	AWStats.Configuration.File.Remote.Command.Execution	medium	server	Windows, Linux	block	CVE-2010-4367	TCP/HTTP
13831	AWStats.Remote.Command.Injection	medium	server	Linux	block	CVE-2006-2237	TCP/HTTP
32186	AWStats.Totals.Sort.Remote.Command.Execution	high	server	Windows, Linux, BSD, Solaris	block	CVE-2008-3922	TCP/HTTP
14341	Aardvark.Topsites.PHP.Remote.Command.Execution	high	server	Windows, Linux, BSD, Solaris	block	CVE-2006-2149, CVE-2006-70	TCP/HTTP
10511	ActivePerl.Perl5.dll.Remote.Buffer.Overflow	low	server	Windows	block	CVE-2001-0815	TCP/HTTP
29585	Adobe.Acrobat.AcroPDF.DLL.Remote.DoS	high	client	Windows	block	CVE-2006-6236	TCP/HTTP
17794	Adobe.Acrobat.Firefox.Plugin.Remote.Code.Execution	critical	client	Windows	block	CVE-2009-2991	TCP/HTTP
44942	Adobe.Acrobat.IP22.Channel.Computation.Remote.Code.Execution	high	server/client	Windows, MacOS	block	CVE-2017-16400	TCP/HTTP/TFTP/SMTP
44941	Adobe.Acrobat.XPS.Glyph.Render.Transform.Remote.Code.Execution	high	server/client	Windows, MacOS	block	CVE-2017-16399	TCP/HTTP/TFTP/SMTP
48262	Adobe.ColdFusion.JNBridge.Binary.Protocol.Remote.Code.Execution	critical	server	All	block	CVE-2019-7839	TCP
37951	Adobe.Flash.AVM2.Remote.Code.Execution	critical	server/client	All	block	CVE-2014-0497	TCP/HTTP/TFTP/SMTP
43637	Adobe.Flash.Audio.Handling.Out.Of.Bounds.Remote.Code.Execution	critical	server/client	Windows, Linux, MacOS	block	CVE-2015-5577	TCP/HTTP/TFTP/SMTP

11. Click the **Add Filter** button to add a filter.

The screenshot shows the 'Policy & Objects' interface with the 'Object Configurations' tab selected. The 'OS = MacOS' filter is applied. The 'IPS Signatures' list is displayed, showing various signatures with their names, severities, targets, and actions. The filter is applied to the list.

ID	Name	Severity	Target	OS	Action	CVE-ID	Protocol
47982	74CMS.Config.Controller.Remote.Code.Execution	critical	server	Windows, Linux, BSD, Solaris	block	CVE-2019-10684	TCP/HTTP
27400	A-Link.WL54AP3.And.WL54AP2.goform.CSRF	low	client	All	block	CVE-2008-6823	TCP/HTTP
38015	A325.Botnet	critical	server/client	All	block		TCP
40473	AAEH.Botnet	critical	server	All	block		UDP/DNS
37624	AARC.Botnet	critical	client	All	block		TCP
39088	ABNR.Botnet	critical	server	All	block		TCP/HTTP
14343	ACal.Arbitrary.Command.Execution	low	server	Windows, Linux, BSD, Solaris	block	CVE-2006-2261	TCP/HTTP
15544	ACal.Calendar.Cookie.Based.Authentication.Bypass	high	server	Windows, Linux, BSD, Solaris	block	CVE-2006-0182	TCP/HTTP
39648	ADKR.Botnet	critical	server	All	block		TCP/HTTP
18149	AJ.Dating.Viewprofile.PHP.SQL.Injection	high	server	Windows, Linux, BSD, Solaris	block	CVE-2007-1297	TCP/HTTP
41735	AIQ.Botnet	critical	server	All	block		TCP/HTTP
27599	AOL.Picture.Editor.YGPPicEdit.ActiveX.Control.Buffer.Overflow	low	client	Windows, Linux, MacOS	block	CVE-2007-6699	TCP/HTTP
27241	APC.PowerChute.Network.Shutdown.HTTP.Response.Splitting	medium	server	All	block		TCP/HTTP
34792	APT1.SSL.Certificate	medium	client	All	block		TCP/SSL
26832	ASX.Playlist.HREF.Buffer.Overflow	high	client	All	block	CVE-2017-15083	TCP/HTTP
42238	ATutor.MOD.PHP.ZIP.File.Upload.Directory.Traversal	high	server	All	block	CVE-2019-12169	TCP/HTTP
42237	ATutor.MOD.connections.php.SQL.Injection	critical	server	All	block	CVE-2016-2555	TCP/HTTP
31505	AUTH.TLS.Plaintext.Command.Injection	high	server	All	block	CVE-2011-1575	TCP/FTP
32186	AWStats.Totals.Sort.Remote.Command.Execution	high	server	Windows, Linux, BSD, Solaris	block	CVE-2008-3922	TCP/HTTP
27321	AWStats.awstats.PLURL.Handling.XSS	low	server	All	block	CVE-2008-3714	TCP/HTTP
14341	Aardvark.Topsites.PHP.Remote.Command.Execution	high	server	Windows, Linux, BSD, Solaris	block	CVE-2006-2149, CVE-2006-70	TCP/HTTP
49574	Acrobat.Acrobat.Reader.CVE-2020-24434.Out.Of.Bounds.Read	high	server/client	Windows, MacOS	block	CVE-2020-24434	TCP/HTTP/TFTP/SMTP
49571	Acrobat.Reader.Acrobat.CVE-2020-24433.Arbitrary.File.Creation	high	server/client	Windows, MacOS	pass	CVE-2020-24433	TCP/HTTP/TFTP/SMTP

12. To clear search terms and filters, click **Reset Search** and **Reset Filters** buttons.

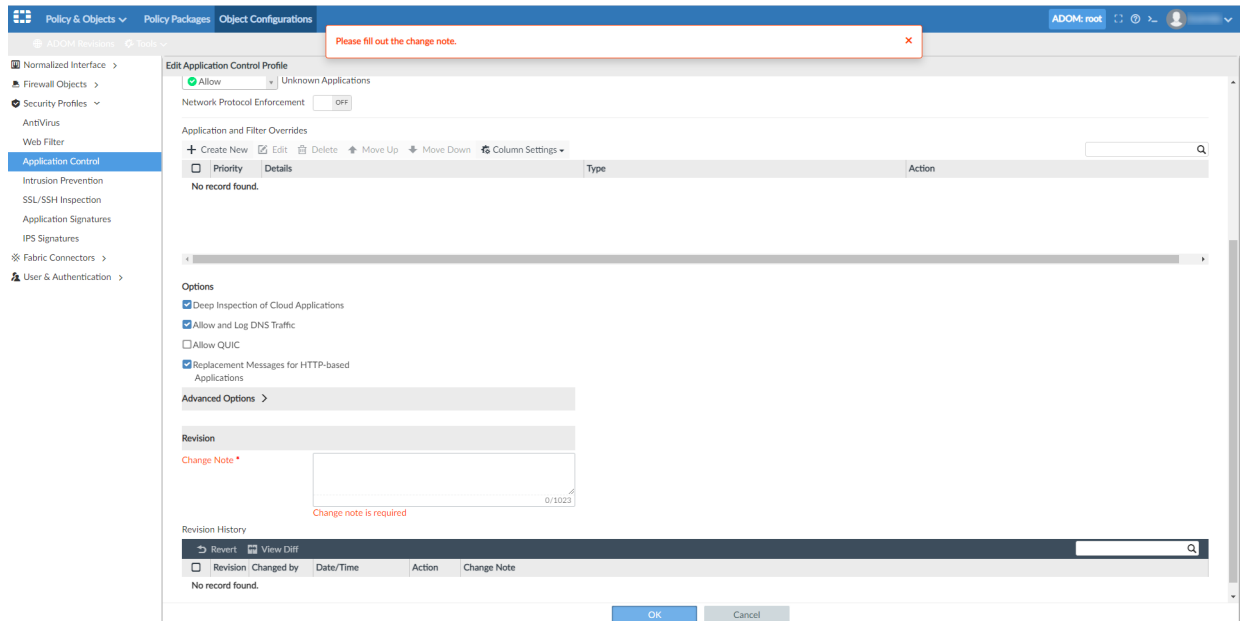
Object revision history

You are now required to provide a **Change Note** when you create or edit an object. You can also use the new **Revision History** table to revert a change or compare versions of an object.

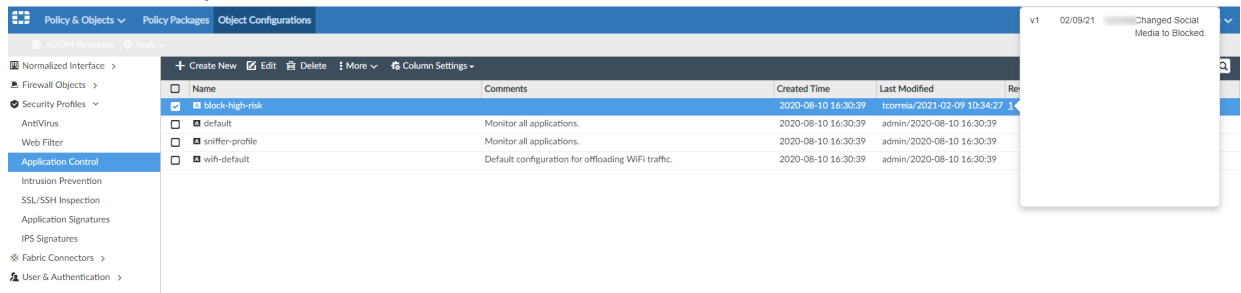
To view the revision history:

1. Go to **Policy & Objects > Object Configurations**.
2. Double-click an object to edit it.

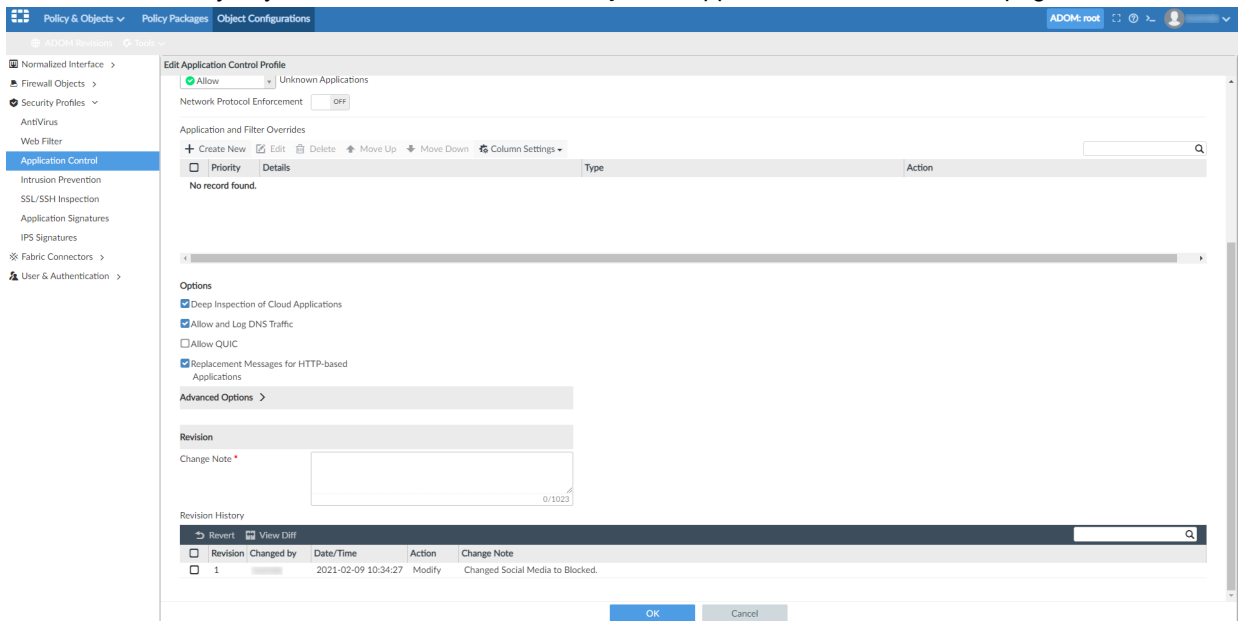
3. Revise the object, and then enter a description in the *Change Note* field. You cannot save your changes until you provide a change note.



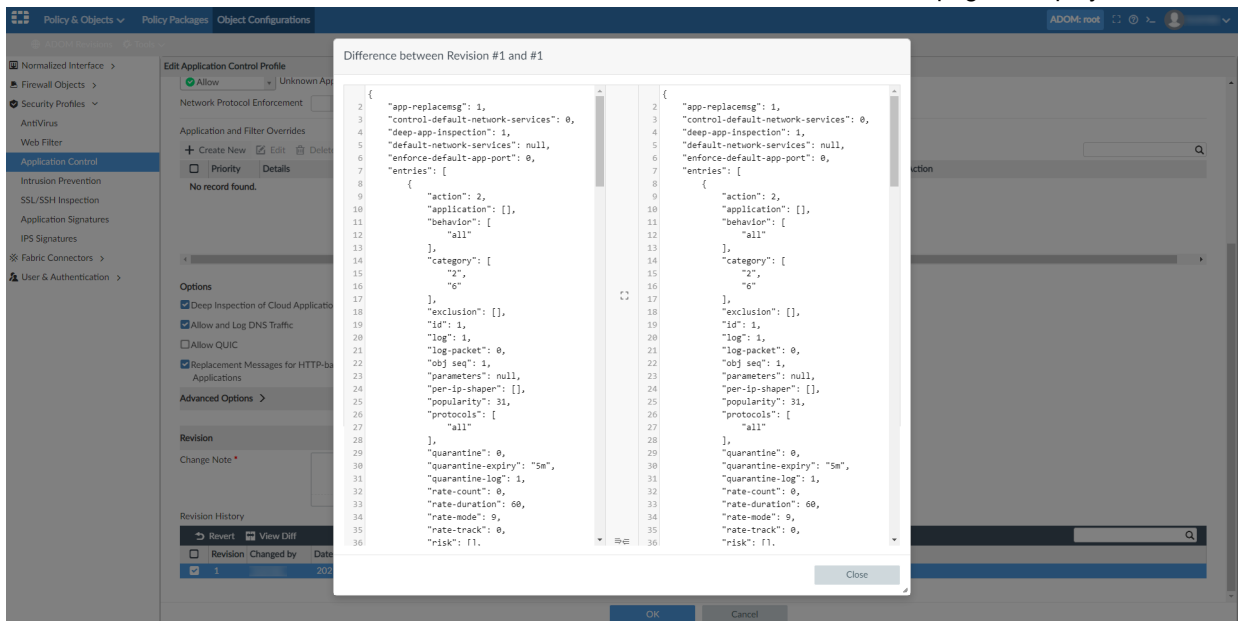
4. Click **OK**. The number of revisions are displayed in the *Revision History* column. Click the link in the column to view the revision history.



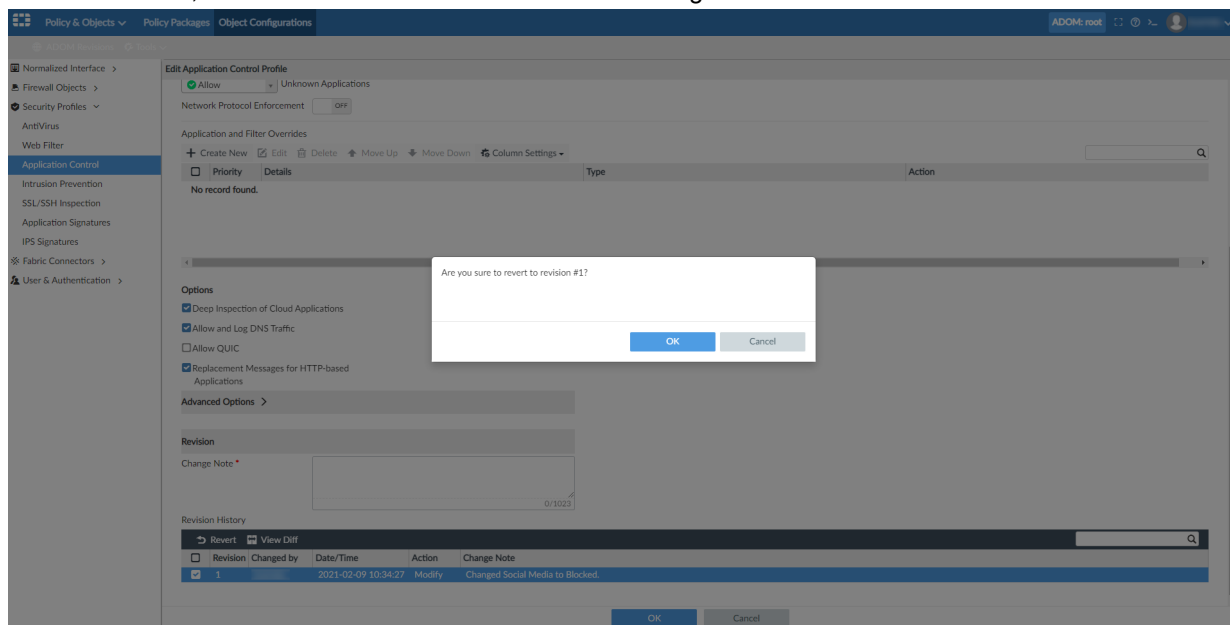
5. Double-click the object you edited. The *Revision History* table appears at the bottom of the page.



6. Select a revision, and click *View Diff*. The *Difference between Revision <#> and <#>* page is displayed.



7. Select a revision, and click *Revert*. Click *OK* to revert the change.



System

This section lists the new features added to FortiManager for system settings:

- [High Availability \(HA\) on page 96](#)
- [Administrators on page 99](#)
- [ADOM on page 106](#)

High Availability (HA)

This section lists the new features added to FortiManager for high availability (HA):

- [FortiManager verifies if FortiAnalyzer features are disabled before forming HA cluster on page 96](#)
- [Cluster HA improvements 7.0.1 on page 98](#)

FortiManager verifies if FortiAnalyzer features are disabled before forming HA cluster

With FortiManager 7.0.0, you cannot enable FortiAnalyzer features on FortiManager nodes that are part of an HA cluster.

If FortiAnalyzer features are enabled on FortiManager nodes in an HA cluster before you upgrade to FortiManager 7.0.0, FortiAnalyzer features are automatically disabled on each FortiManager in the HA cluster during upgrade.

After upgrading to FortiManager 7.0.0, you cannot enable FortiAnalyzer features on any FortiManager nodes that are part of an HA cluster, and the *FortiAnalyzer Features* option is hidden in the GUI.

For standalone FortiManager units with FortiAnalyzer features enabled, you must disable FortiAnalyzer features before you can form a FortiManager HA cluster after upgrading to FortiManager 7.0.0.

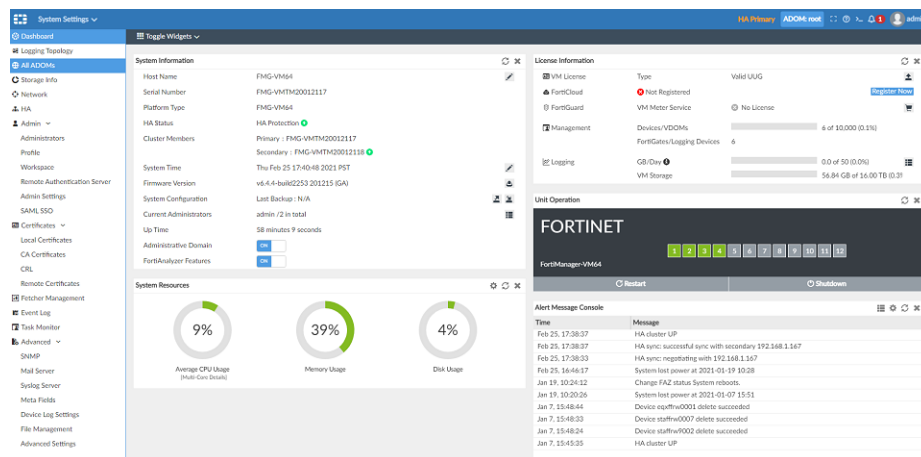
This topic contains the following sections:

- [FortiAnalyzer features disabled during upgrade on page 96](#)
- [FortiAnalyzer features disabled when HA enabled on page 97](#)
- [FortiAnalyzer features disabled before forming HA on page 97](#)

FortiAnalyzer features disabled during upgrade

If FortiAnalyzer features are enabled before you upgrade to FortiManager 7.0.0, FortiAnalyzer features will be automatically disabled during upgrade to FortiManager 7.0.0.

For example, FortiAnalyzer features are enabled on FortiManager before upgrading to FortiManager 7.0.0. On the *System Settings > Dashboard* pane, the *System Information* widget shows *FortiAnalyzer Features* toggled *ON*.

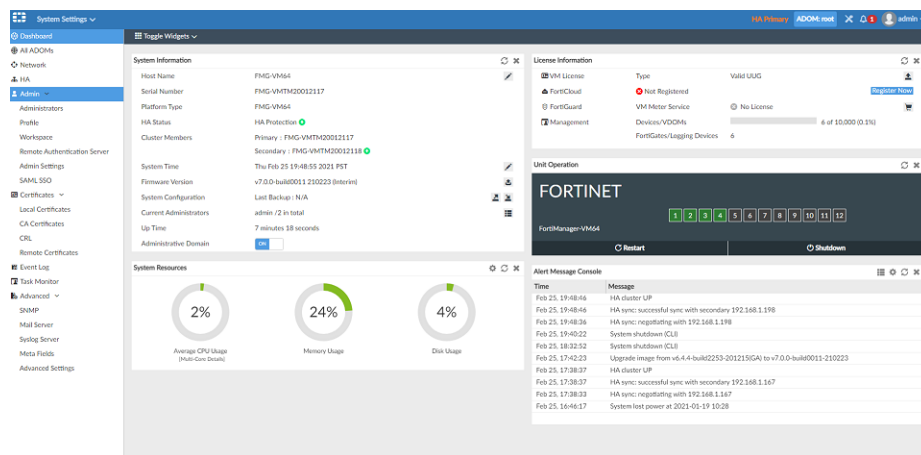


After the upgrade to FortiManager 7.0.0 completes, FortiAnalyzer features are disabled, and the *FortiAnalyzer Features* option is hidden from the GUI.

FortiAnalyzer features disabled when HA enabled

After upgrading to FortiManager 7.0.0, you cannot enable FortiAnalyzer features on any FortiManager nodes that are part of an HA cluster.

In the GUI, the *FortiAnalyzer Features* option is hidden:



In the CLI, an error message is displayed if you try to enable FortiAnalyzer features:

```
FMG-VM64 # config system global
(global)# set faz-status enable
(global)# end
```

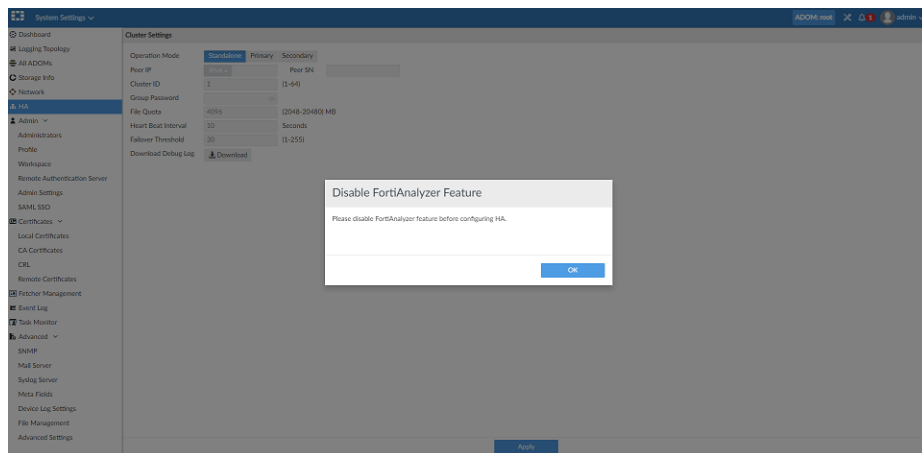
Please disable HA before enabling FortiAnalyzer feature.
object set operator error, -7 discard the setting
Command fail. Return code -7

FortiAnalyzer features disabled before forming HA

When FortiAnalyzer features are enabled on FortiManager in stand-alone mode, you cannot form an HA cluster.

When you try to form an HA cluster, FortiManager checks each FortiManager node for enabled FortiAnalyzer features.

In the GUI, when enabled FortiAnalyzer features are found, a message is displayed, asking you to disable FortiAnalyzer features first:



In the CLI, when you try to enable HA mode, an error message is displayed, asking you to disable FortiAnalyzer features first:

```
FMG-VM64 # config system ha
(ha)# set mode primary
(ha)# end
Please disable FortiAnalyzer feature before enabling HA.
object set operator error, -7 discard the setting
Command fail. Return code -7
FMG-VM64 #
FMG-VM64 # config system ha
(ha)# set mode secondary
(ha)# end
Please disable FortiAnalyzer feature before enabling HA.
object set operator error, -7 discard the setting
Command fail. Return code -7
FMG-VM64 #
```

When FortiManager detects disabled FortiAnalyzer features on each FortiManager node, you can form a FortiManager HA cluster by using the GUI or the CLI.

Cluster HA improvements - 7.0.1

FortiManager 7.0.1 includes the following cluster HA improvements: cluster status, last sync, and on-demand/on-schedule HA nodes integrity check.

To configure an on-schedule HA integrity check:

```
config system ha-schedule-check
set status {enable | disable}
set week_days {monday | tuesday | wednesday | thursday | friday | saturday | sunday}
set time <hh.mm.ss>
end
```

To run an on-demand HA integrity check:

```
diagnose ha check-data {start | stop | status}
```

To check the integrity check report:

```
diagnose ha data-check-report
```

Example:

```
config system ha-scheduled-check
  set status enable
  set week_days monday
  set time "15:53:10"
end
diagnose ha data-check-report
Data check starts at Mon Jul 26 15:53:19 2021
--- Unit FMG-VM0A17002226 ---
All data files matched
Data check done at Mon Jul 26 15:53:23 2021
```

Administrators

This section lists the new features added to FortiManager for administrators:

- [Theme mode on page 99](#)
- [Admin Permission to enable/disable script tab access on page 100](#)
- [Admins can use a SAML SSO FortiCloud account to log in to FortiManager on page 102](#)

Theme mode

When you create a new user, you can to apply a theme to all the administrator accounts, or allow admins to choose their own theme

To enable themes per admin:

1. Go to *Admin > Administrators*.
2. In the toolbar, click *Create New*. The *New Administrator* page is displayed.

3. Set *Theme Mode* to *Use Own Theme*.

4. From the *User Theme* menu, select a theme.

New Administrator

User Name: Admin

Avatar: + Change Photo - Remove Photo

Comments:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted User

Administrative Domain: All ADOMs All ADOMs except specified ones: Specify

JSON API Access: None

Trusted Hosts: OFF

Theme Mode: Use Global Theme Use Own Theme

User Theme:

Blueberry	Kiwi	Cherry	Plum
Spring	Summer	Autumn	Winter
High Contrast Dark	Space	Calla Lily	Binary Tunnel
Diving	Dreamy	Technology	Landscape
Twilight	Canyon	Northern Light	Astronomy
Fish	Penguin	Mountain	Polar Bear
Parrot	Cave	Zebra	

Meta Fields >

Advanced Options >

5. Click OK.

When a user logs into their account, they can change the theme by clicking their username, and selecting *Change Profile*.

Change Profile

Change Avatar: Select a photo from your computer

Theme Mode: Use Global Theme Use Own Theme

Theme:

Blueberry	Kiwi	Cherry	Plum
Spring	Summer	Autumn	Winter
High Contrast Dark	Space	Calla Lily	Binary Tunnel
Diving	Dreamy	Technology	Landscape
Twilight	Canyon	Northern Light	Astronomy
Fish	Penguin	Mountain	Polar Bear
Parrot	Cave	Zebra	

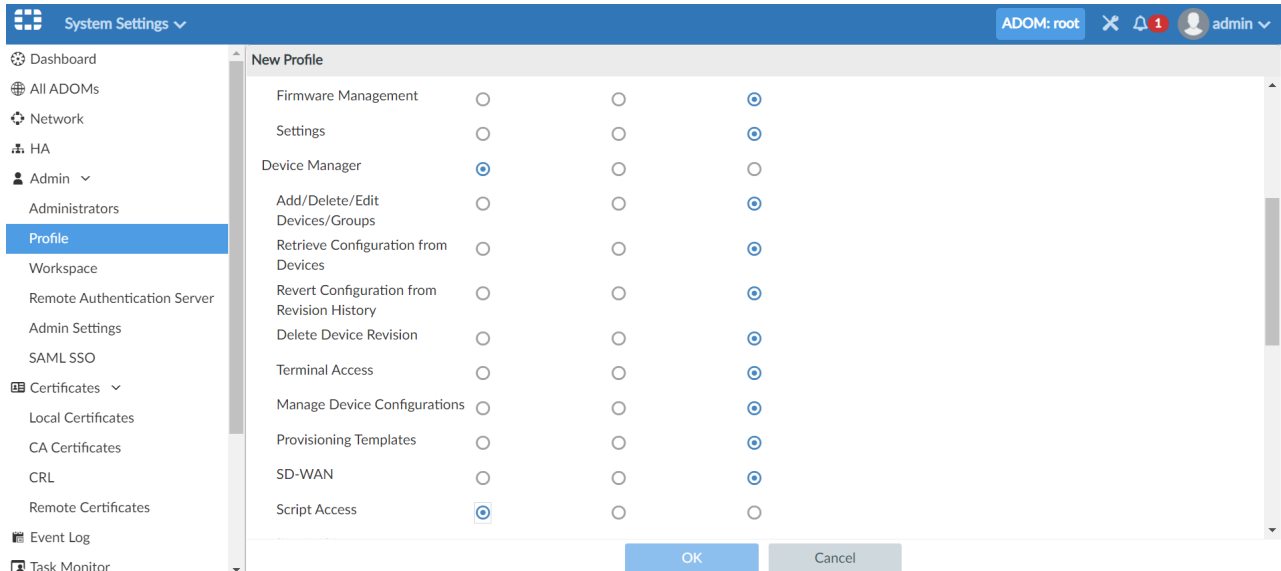
OK Cancel

Admin Permission to enable/disable script tab access

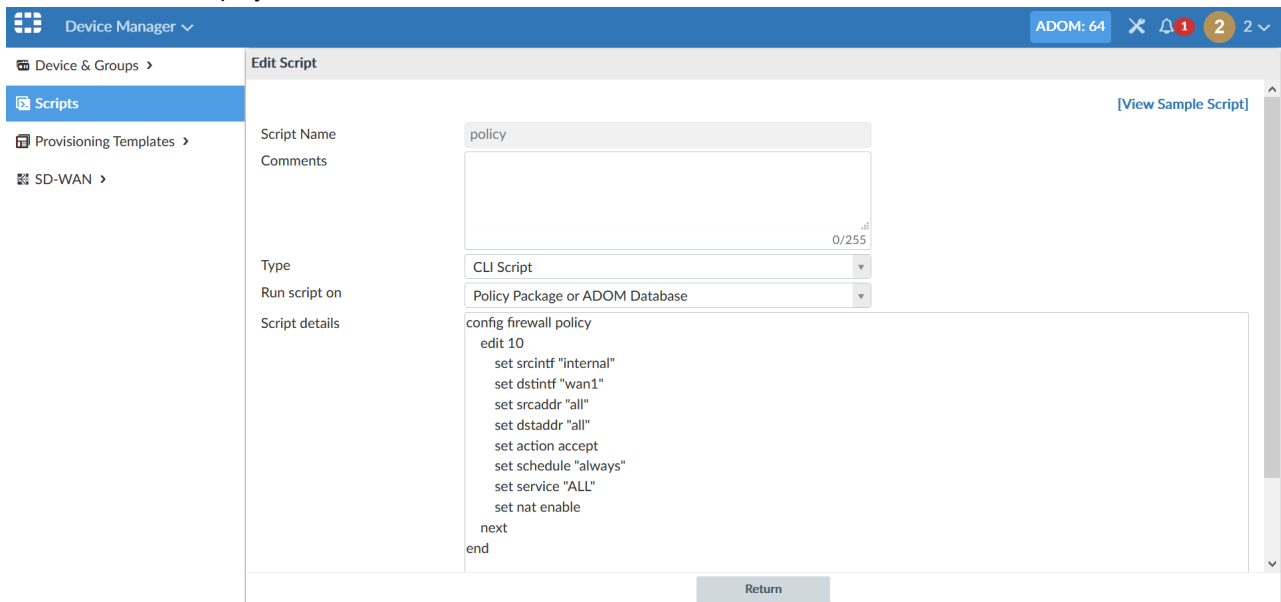
User profiles now contain a *Script Access* setting to allow administrators to create, edit, or delete a script. Users with *read-write* and *read-only* privileges will see the *Scripts* tab in the tree-menu at the left side of the page.

To enable Script Access:

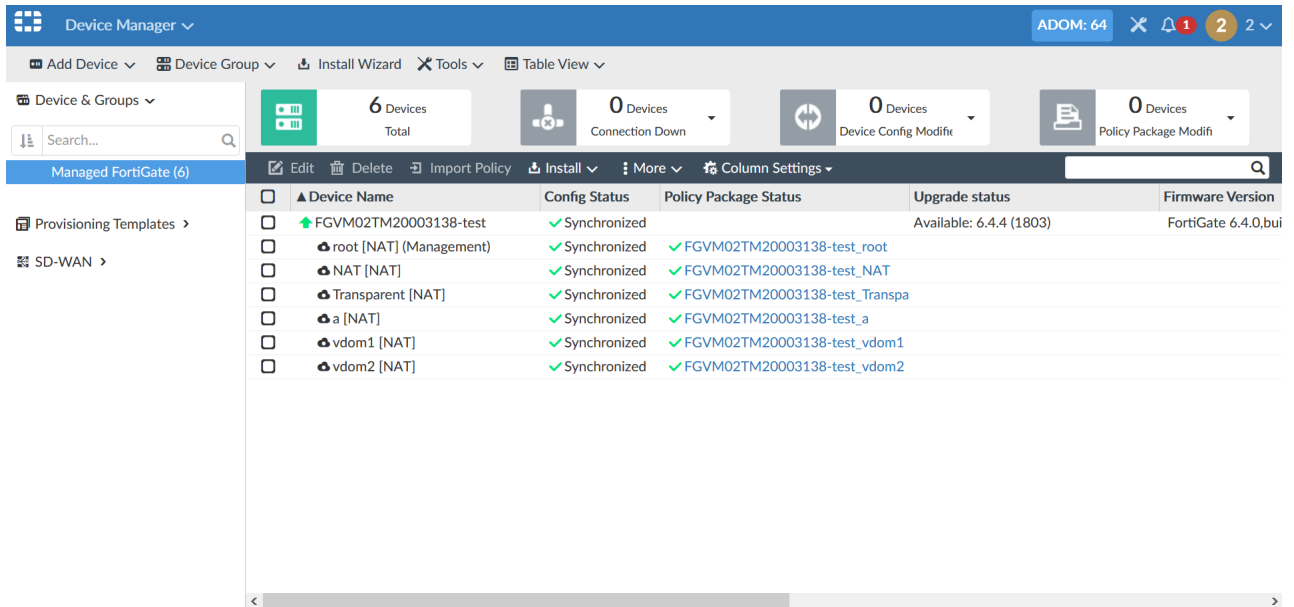
1. Go to **System Settings > Admin > Profile**. The **Script Access** setting is located in the **Device Manager** section.



2. Set **Script Access** to **Read-Write**, and click **OK**. The **Scripts** module is displayed in the tree-menu.
3. When the setting is set to **Read-Only**, the user can see scripts but cannot create, edit, or delete a script. The **Return** button is displayed.



4. When the setting is set to *None*, the *Script* tab does not appear in the tree-menu.

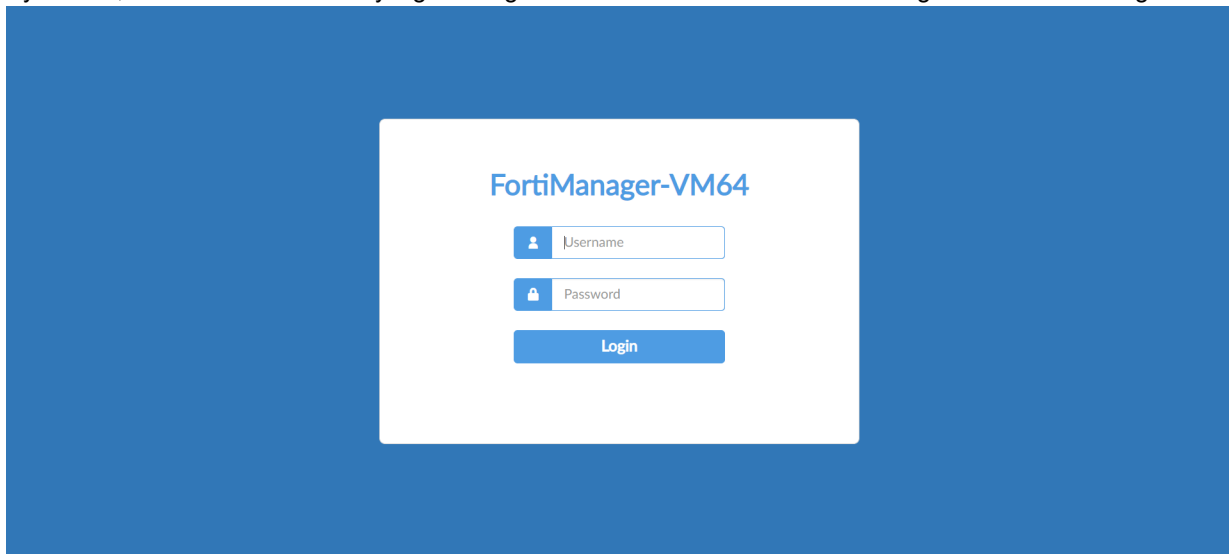


Admins can use a SAML SSO FortiCloud account to log in to FortiManager

Admins can use SAML SSO through their FortiCloud account to log in to FortiManager.

To enable SAML SSO using FortiCloud:

1. By default, administrators can only log in using a local or remote user account configured on FortiManager.



2. To enable SAML SSO using FortiCloud, you must first register your FortiManager on [FortiCloud](#). You can confirm the FortiCloud registration status in *System Settings > Dashboard* under *License Information*.

The screenshot shows the FortiManager System Settings Dashboard. The left sidebar contains navigation options: Dashboard, All ADOMs, Network, HA, Admin (with sub-items: Administrators, Profile, Workspace, Remote Authentication Server, Admin Settings, SAML SSO), Certificates (with sub-items: Local Certificates, CA Certificates, CRL, Remote Certificates), Event Log, and Task Monitor. The main content area is divided into two panels. The 'System Information' panel displays details such as Host Name (FMG-VM64), Serial Number (FMG-VM642100089), Platform Type (FMG-VM64), HA Status (Standalone), System Time (Mon Mar 15 13:37:01 2021 PDT), Firmware Version (v7.0.0-build0019 210311 (Interim)), System Configuration (Last Backup : N/A), Current Administrators (admin / 1 in total), Up Time (2 days 21 hours 16 minutes), Administrative status (ON), Domain, FortiAnalyzer (OFF), and Features. The 'License Information' panel shows a table of licenses:

VM License	Type	Valid UUG
FortiCloud	Registered	
FortiGuard	VM Meter Ser...	No License
Management	Devices/VDO...	1 of 10,000 (0)
Update	AntiVirus and I...	96.45.33.86 Sunnyvale, Calif...
Server	Web and Email...	96.45.33.64 Sunnyvale, Calif...
	FortiClient Up...	96.45.33.106 Sunnyvale, Calif...

Below the license table is a 'Unit Operation' section with a 'FORTINET' logo and a status bar.

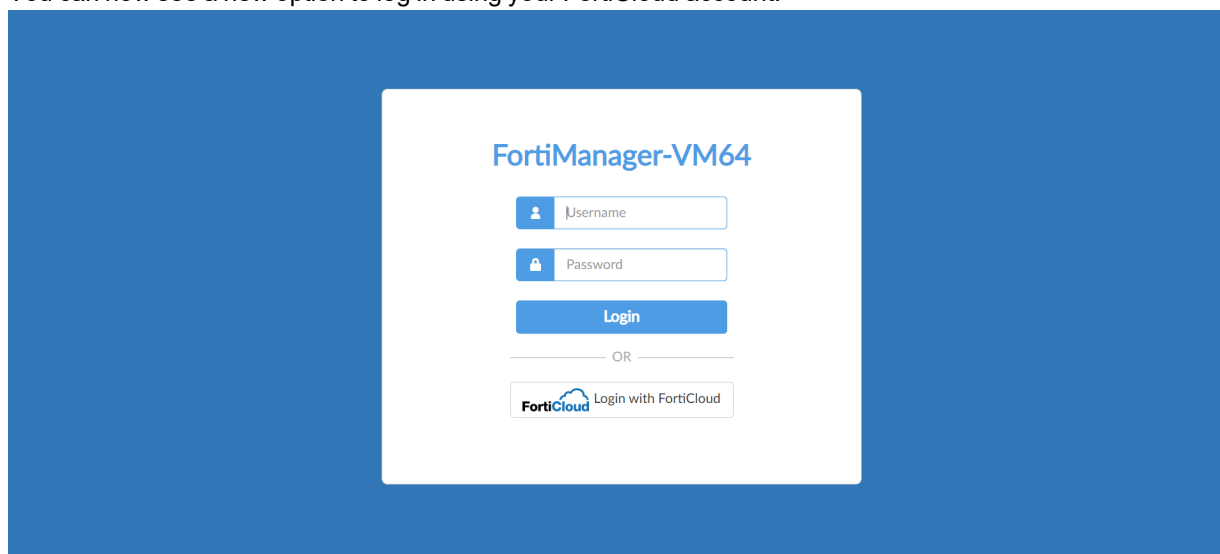
3. Go to *System Settings > Admin > SAML SSO*, and set the *Allow admins to login with FortiCloud* toggle to the ON position. Click *Apply*.

The screenshot shows the FortiManager System Settings SAML SSO configuration page. The left sidebar is the same as in the previous screenshot, but 'SAML SSO' is selected. The main content area is titled 'Single Sign-On Settings' and contains the following fields:

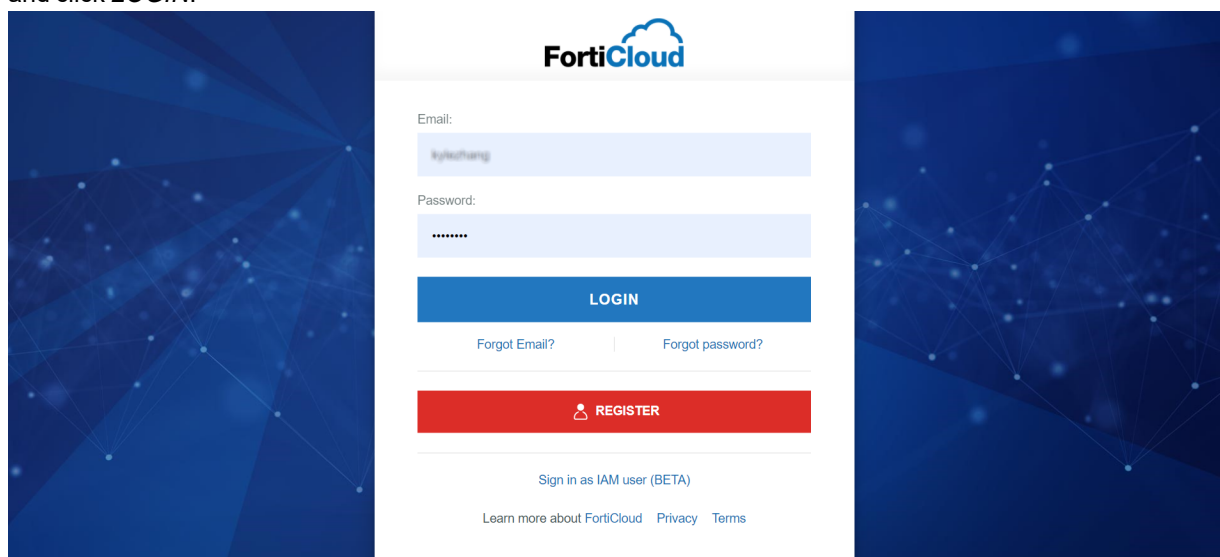
- Server Address: 10.2.116.125
- Allow admins to login with FortiCloud: ☒ ON
- Single Sign-On Mode: Disabled (selected), Identity Provider (IdP), Service Provider (SP)

An 'Apply' button is located at the bottom right of the configuration area.

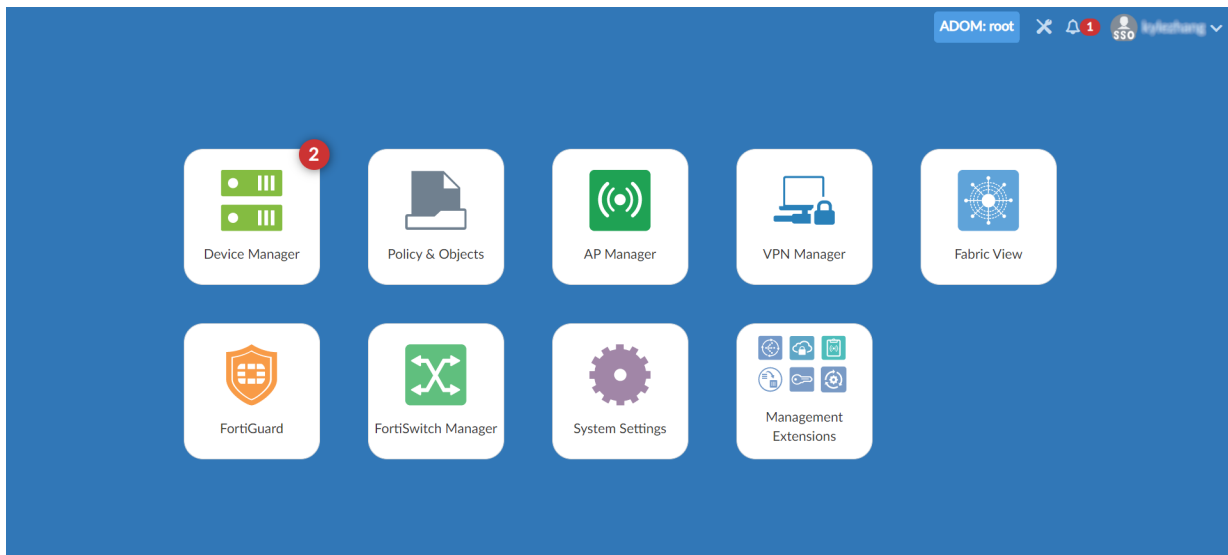
4. Sign out of FortiManager and return to the login page.
You can now see a new option to log in using your FortiCloud account.



5. Click *Login with FortiCloud* and you are redirected to the FortiCloud login portal. Enter your FortiCloud credentials, and click *LOGIN*.

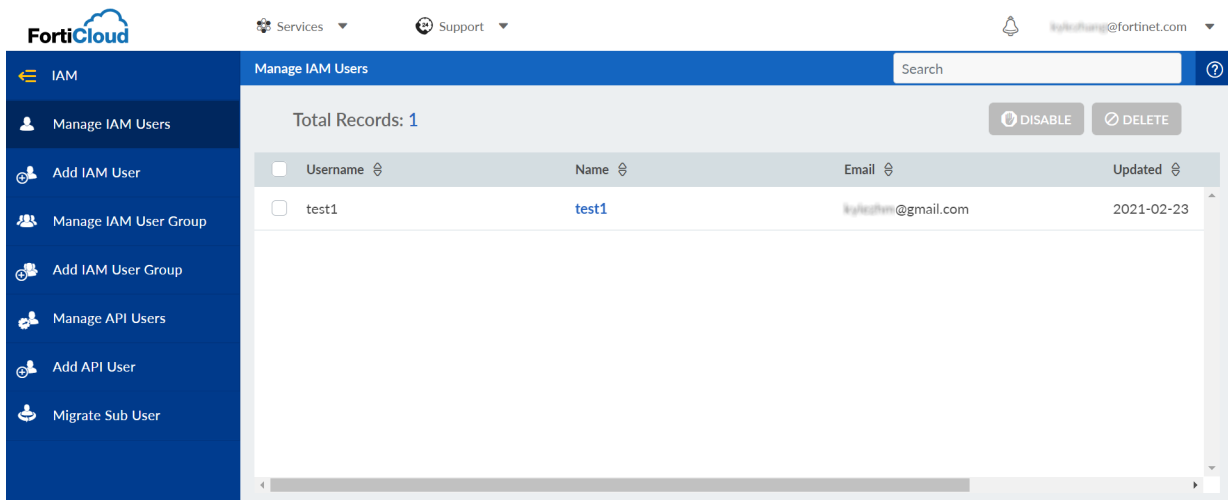


You are logged in to FortiManager with your FortiCloud account.

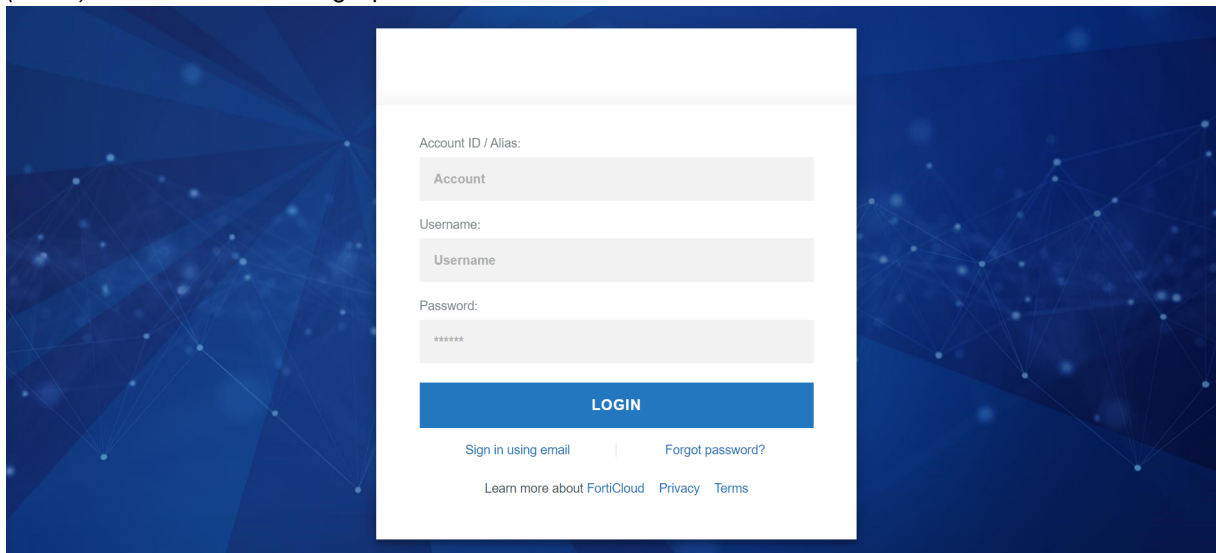


By default, only the account ID which the FortiManager is registered to can be used to log in to FortiManager. To enable login for additional user accounts using FortiCloud, you can configure multiple IAM users in FortiCloud.

6. Go to FortiCloud and create one or more IAM users. For more information on creating an IAM user, see [Identity & Access Management \(IAM\)](#).



7. Go to the FortiManager sign in page and click *Login with FortiCloud*, and click the option to *Sign in as IAM user (BETA)* at the bottom of the login portal.



8. Enter your IAM user credentials, and you will be logged in to FortiManager as the IAM user.

ADOM

This section lists the new features added to FortiManager for ADOMs:

- [ADOM health check tool reports warnings on devices, configurations, and policy package status on page 106](#)
- [Managing mixed FortiOS versions 6.2 and 6.4 in a single ADOM on page 109](#)
- [Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM 7.0.1 on page 112](#)
- [ADOM upgrade from 6.4 to 7.0 7.0.1 on page 114](#)

ADOM health check tool reports warnings on devices, configurations, and policy package status

From the *System Settings > All ADOMs* pane, you can check the status of all devices in all ADOMs. You can check the status of the following criteria for all devices in all ADOMs:

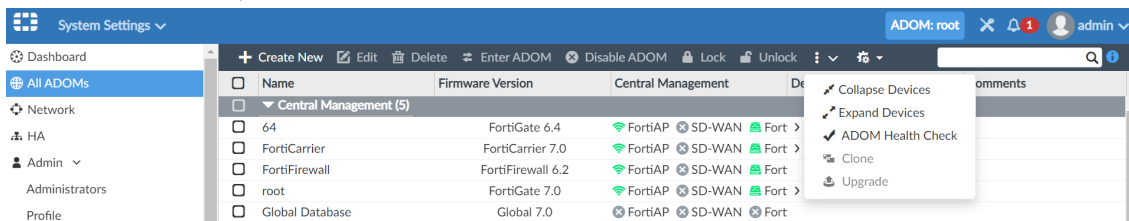
- Device connection is down.
- Device configuration status is not synchronized.
- Device policy package status is not synchronized.

You can also choose whether to exclude model devices from the health check.

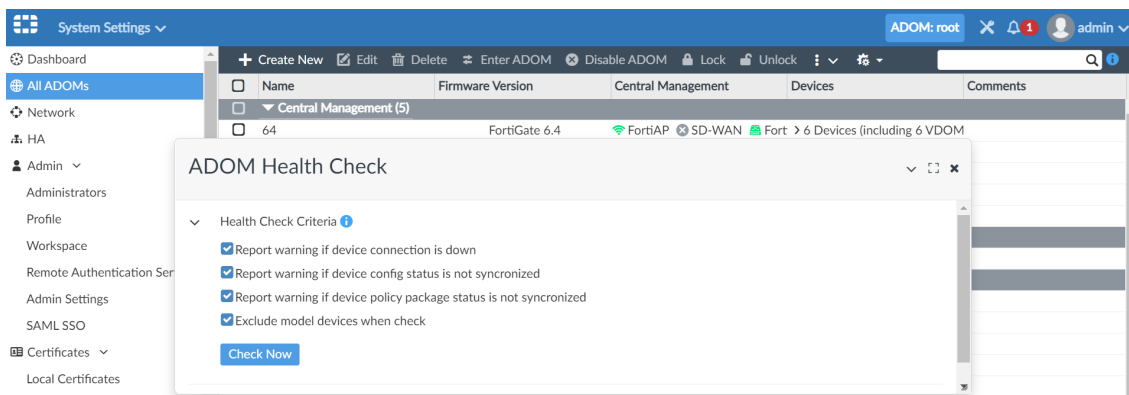
When the health check status is displayed, you can view what ADOMs contain problematic devices, and go directly to the *Device Manager* pane in the ADOM with problematic devices. You can also return to the *ADOM Health Check* dialog box, and continue checking ADOM statuses.

To check ADOM health:

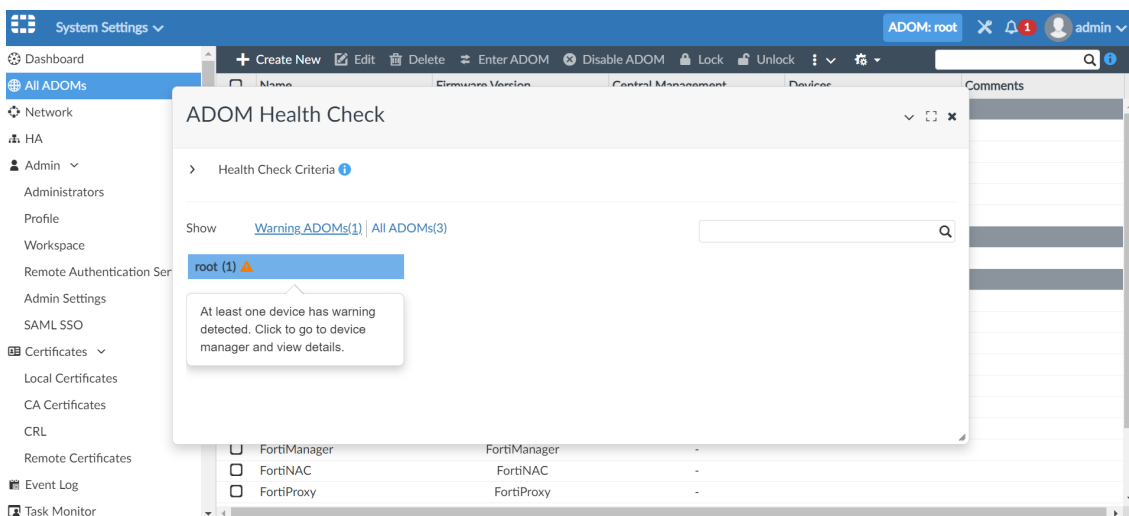
1. Go to *System Settings > All ADOMs*.
2. From the *More* menu, select *ADOM Health Check*.



The *ADOM Health Check* dialog box is displayed.

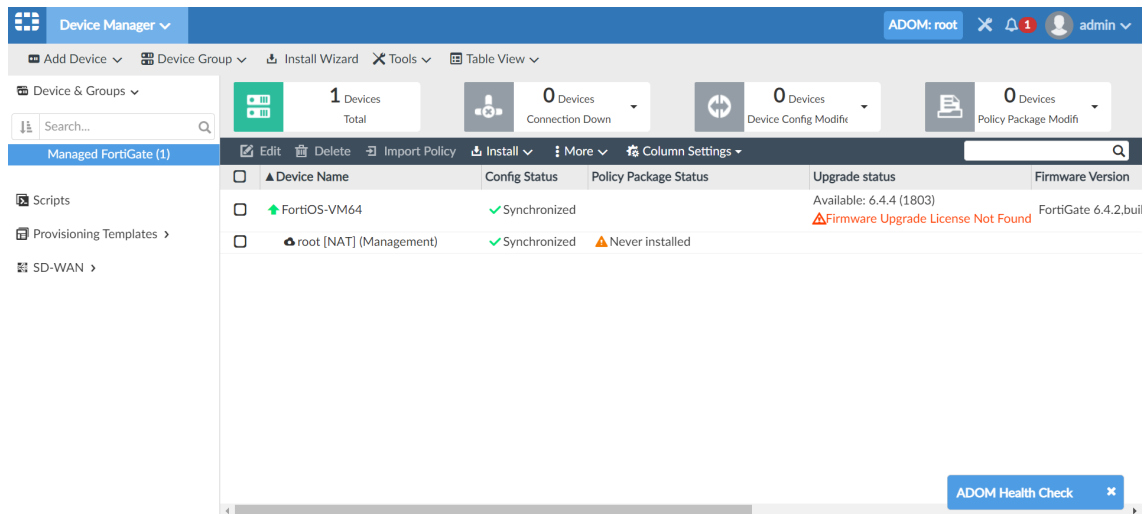


3. In the *Health Check Criteria* section, select what criteria to check, and click *Check Now*.
The results of the check are displayed. In the following example, *Warning ADOMs <number>* is selected, and the list of ADOMs with warnings are displayed. The *root* ADOM has a warning.

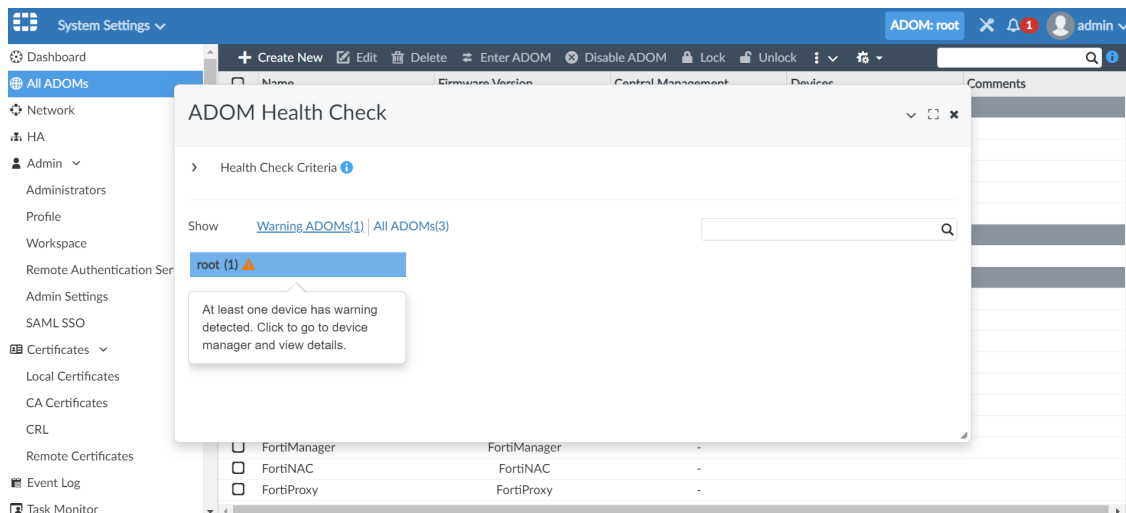


4. Under *Warning ADOMs <number>*, click *root <number>* to display the *Device Manager* pane, and view details about the warning.

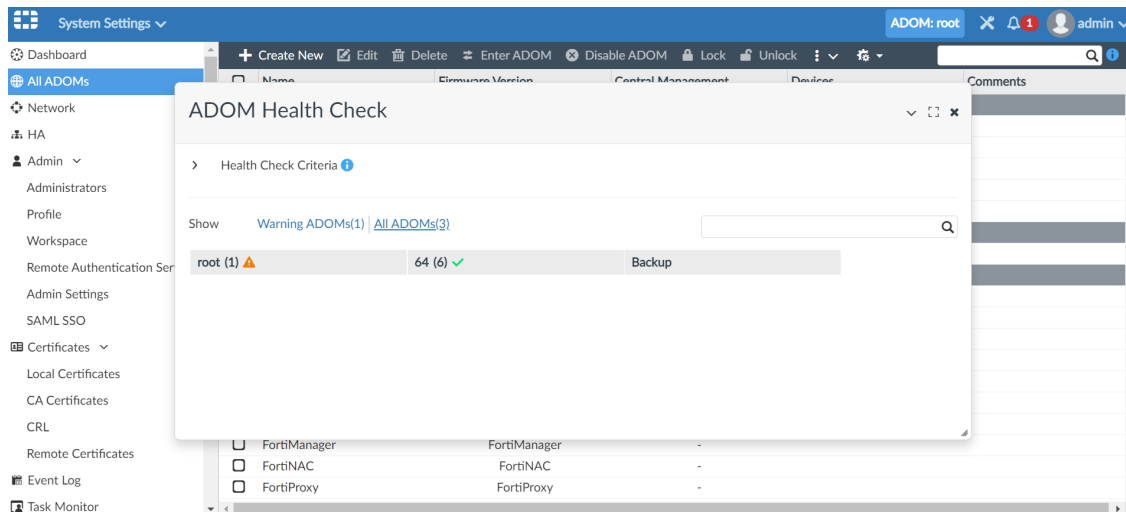
The *Device Manager* pane is displayed for the ADOM with the warning. The *ADOM Health Check* button remains at the bottom of the pane.



5. At the bottom-right of the *Device Manager* pane, click the *ADOM Health Check* button to return to the *ADOM Health Check* dialog box, and continue checking ADOMs. The *ADOM Health Check* dialog box is displayed.



6. Click *All ADOMs <number>*.
A summary of all ADOMs is displayed. In the following example, a warning status (orange triangle) displays beside the *root* ADOM, and a synchronized status (green checkmark) displays beside the *64* ADOM.



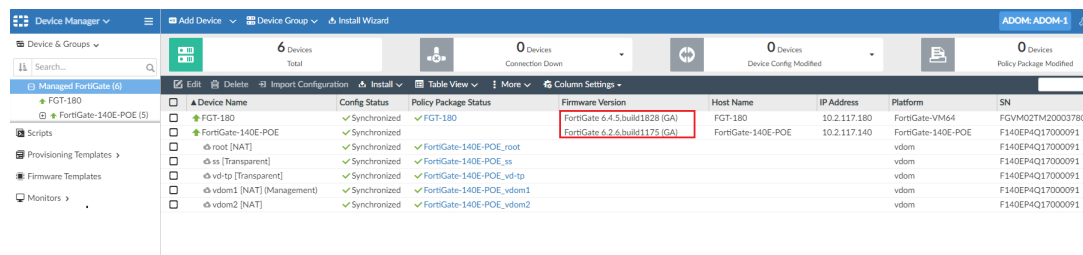
- Click the x on the top-right corner to close the dialog box.

Managing mixed FortiOS versions 6.2 and 6.4 in a single ADOM

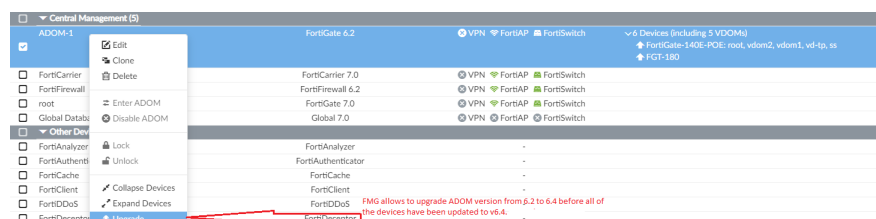
FortiManager ADOM version 6.2 can concurrently manage FortiGate units running FortiOS 6.2.x and FortiOS 6.4.x. You can now upgrade ADOM version 6.2 to 6.4 before upgrading all FortiGates in the ADOM to FortiOS 6.4.x.

After you upgrade the ADOM to version 6.4, you can install policy package version 6.4 to FortiGates in the ADOM running FortiOS 6.4.x and FortiOS 6.2.x. FortiManager automatically downgrades the CLI to version 6.2 for FortiGate devices in the ADOM running FortiOS 6.2.x.

In the following example, an ADOM version 6.2 named *ADOM-1* contains a mix of FortiGates running version 6.4.x and 6.2.x:



However, you can right-click *ADOM-1*, and select *Upgrade* to upgrade the ADOM from version 6.2 to 6.4:



After upgrading the ADOM from version 6.2 to 6.4, features for ADOM version 6.4 are available. The following example of the *Policy & Objects* pane is for ADOM version 6.2:

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
1		port24 port28 port26 port30 port26-v100	wan1	all	all	always	ALL		Accept	no-inspection default	Log
2		wifi2	wan1	all	all	always	ALL		Accept	certificate-inspect default	Log
3		stability3	wan1	all	all	always	ALL		Accept	g-default certificate-inspect default	Log
4	Implicit Deny	any	any	all	all	always	ALL		Deny		No I

ADOM version v6.3 firewall policy IPv4 and IPv6

After upgrading to ADOM version 6.4, the following features are available on the *Policy & Objects* pane:

#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log
5	csp	wifi2	wan1	all	all	always	ALL		Accept	no-inspection default	Log AI
6	port1	port1	wan1	all	all	always	ALL		Accept	no-inspection default	Log Se
7	mgmt	mgmt	port19 sw	all	all	always	ALL		Accept	no-inspection default	Log Se
8	wmm	stability3	wan1	all	all	always	ALL		Accept	g-default certificate-inspect default	Log AI
9	ss	stability4	wan1	all	all	always	ALL		Accept	g-default certificate-inspect default	Log AI
10	zone	wifi_zone	wan1	all	all	always	ALL		Accept	no-inspection default	Log AI
11	mmw	wan1	stability3	all	all	always	ALL		Accept	no-inspection default	Log Se
12	wifi	stability2	wan1	all	all	always	ALL		Accept	no-inspection default	Log AI
13	mgmt-vpn	wifi-vpn	port1	all	all	always	ALL		Accept	no-inspection default	Log Se
14	port1-vpn	port1	wifi-vpn	all	all	always	ALL		Accept	no-inspection default	Log Se
15		port24 port28 port26 port30 port26-v100	wan1	all	all	always	ALL		Accept	no-inspection default	Log AI
16		wifi2	wan1	all	all	always	ALL		Accept	certificate-inspect default	Log AI
17		stability3	wan1	all	all	always	ALL		Accept	g-default certificate-inspect default	Log AI

After ADOM upgraded to v6.4, GUI automatically display ADOM-v6.4 feature

When you install the policy package from ADOM version 6.4 to FortiGates running FortiOS 6.2.x and FortiGates running FortiOS 6.4.x, FortiManager automatically downgrades the 6.4 CLI to 6.2 CLI for FortiGates running FortiOS 6.2.x.

For example, the following policy package is for ADOM 6.4:

Policy Packages ▾

Search...

- FGT-180
- FortiGate-140E-POE_root
- FortiGate-140E-POE_ss
- FortiGate-140E-POE_vd-tp
- FortiGate-140E-POE_vdom1
- Firewall Policy**
- Installation Targets
- FortiGate-140E-POE_vdom2

Object Configurations ▸

Edit Firewall Policy

Name: ADOM v6.4 IPv6

Incoming Interface: any

Outgoing Interface: any

Source Internet Service: OFF

IPv4 Source Address: +

IPv6 Source Address: all

Source User: +

Source User Group: +

FSSO Groups: +

Destination Internet Service: OFF

IPv4 Destination Address: +

IPv6 Destination Address: all

Service: ALL

Schedule: always

Action: Deny **Accept** IPSEC

Inspection Mode: **Flow-based** Proxy-based

Firewall/Network Options

NAT: ☐

Protocol Options: default

Disclaimer Options

Display Disclaimer: OFF

Security Profiles

SSL/SSH Inspection: no-inspection

You can install the policy package to FortiGate devices in ADOM 6.4 running both FortiOS 6.2.x and FortiOS 6.4.x:

Policy & Objects ▾

Policy Packages ▾

Search...

- FGT-180
- FortiGate-140E-POE_root
- FortiGate-140E-POE_ss
- FortiGate-140E-POE_vd-tp
- FortiGate-140E-POE_vdom1
- Firewall Policy**
- Installation Targets
- FortiGate-140E-POE_vdom2

Object Configurations ▸

Policy Package ▾ **Install** ▾ **ADOM Revisions** ▾ **Tools** ▾

+ Create New ▾ Edit ▾ Delete ▾ Section ▾ Policy Lookup ▾ Collapse All ▾ Column Settings ▾

#	Name	From	To	Source	Destination	Schedule	Service
1	ADOM v6.4 IPv6	any	any	all	all	always	ALL
Implicit (2-2 / Total: 1)							
2	Implicit Deny	any	any	all	all	always	ALL

Install Wizard - Policy Package and Device Setting (FortiGate-140E-POE_vdom1)

Please select one or more devices to install (Use checkbox or Ctrl or Shift key for multiple selections)

Device Name	IP Address	Platform
<input checked="" type="checkbox"/> FGT-180	10.2.117.180	FortiGate-VM64
<input checked="" type="checkbox"/> FortiGate-140E-POE	10.2.117.140	FortiGate-140E-POE
<input checked="" type="checkbox"/> vdom1 [NAT] (Management)		vdom

In the preview for both devices, you can view what is installed to each device:

Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM - 7.0.1

FortiManager ADOM version 6.4 can concurrently manage FortiGate units running FortiOS 6.4.x and FortiOS 7.0.x. You can now upgrade ADOM version 6.4 to 7.0 before upgrading all FortiGates in the ADOM to FortiOS 7.0.x.



Although you can use a 6.4 ADOM to manage mixed FortiOS versions, it is recommended to upgrade all FortiGates to FortiOS 7.0.x, and then upgrade the ADOM from version 6.4 to 7.0. See also [ADOM upgrade from 6.4 to 7.0 7.0.1 on page 114](#).

After you upgrade the ADOM to version 7.0, you can install policy package version 7.0 to FortiGates in the ADOM running FortiOS 7.0.x and FortiOS 6.4.x. FortiManager automatically downgrades the CLI to version 6.4 for FortiGate devices in the ADOM running FortiOS 6.4.x.

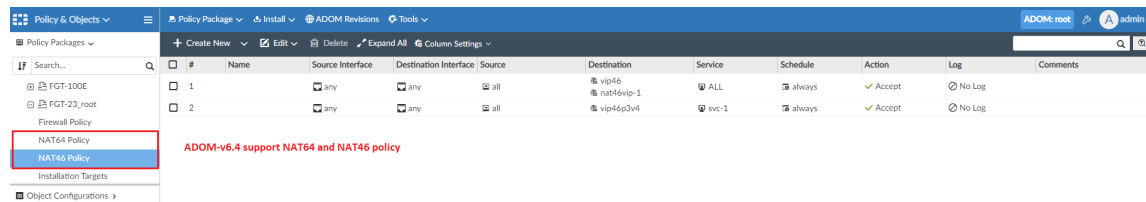
In the following example, an ADOM version 6.4 named *root* contains a mix of FortiGates running version 7.0.x and 6.4.x:

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	Platform	Provisioning Templates	Description
FortiGate 6.4.6.build1879 (GA)	Synchronized	Never installed	FortiGate 6.4.6.build1879 (GA)	FGT-23	FortiGate-VM64	vdom	
FortiGate 7.0.1.build0157 (GA)	Synchronized	Never installed	FortiGate 7.0.1.build0157 (GA)	FGT100	FortiGate-100E	vdom	

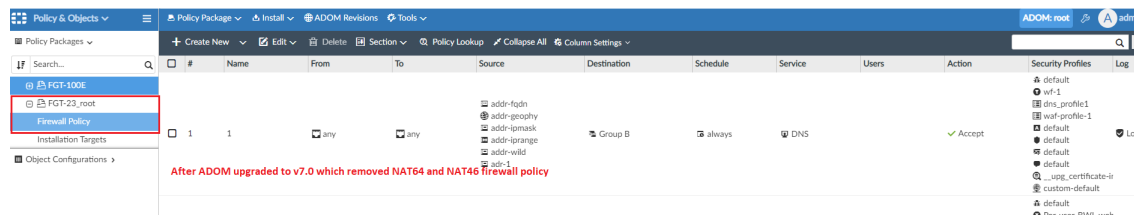
However, you can select *Upgrade* from the *More* menu to upgrade the ADOM from version 6.4 to 7.0:

Name	Firmware Version	Actions
FortiCarrier	FortiCarrier 6.4	Clone, Upgrade, Collapse Devices, Expand Devices, ADOM Health Check
FortiFirewall	FortiFirewall 6.2	Clone, Upgrade, Collapse Devices, Expand Devices, ADOM Health Check
root	FortiGate 6.4	Clone, Upgrade, Collapse Devices, Expand Devices, ADOM Health Check

After upgrading the ADOM from version 6.4 to 7.0, features for ADOM version 7.0 are available. The following example of the *Policy & Objects* pane is for ADOM version 6.4:

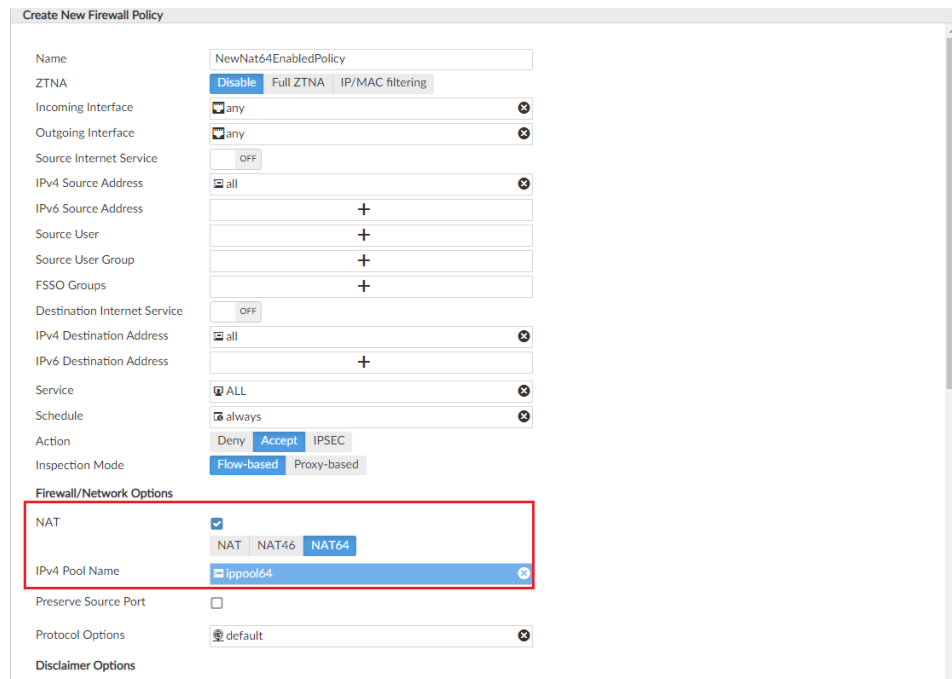


After upgrading to ADOM version 7.0, the following features are available on the *Policy & Objects* pane:

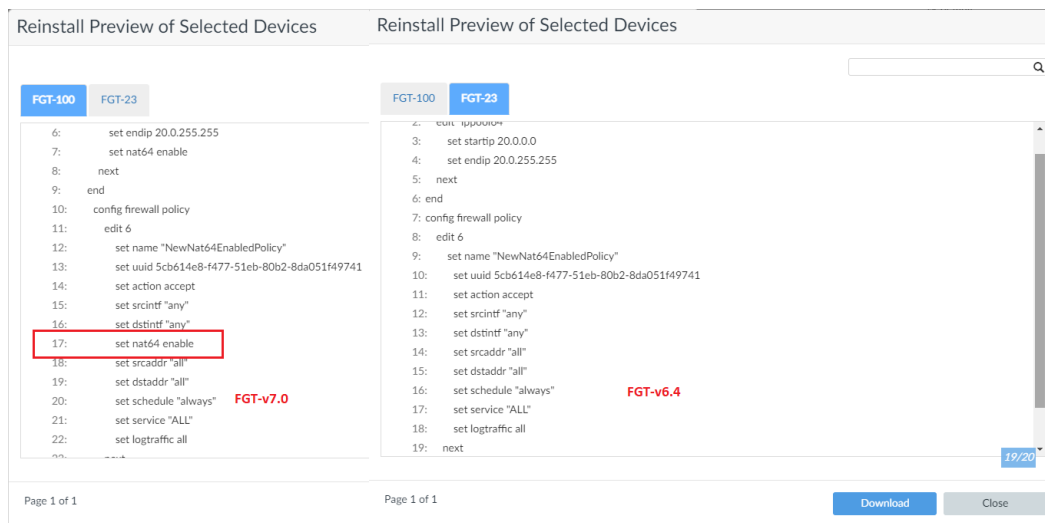


When you install the policy package from ADOM version 7.0 to FortiGates running FortiOS 6.4.x and FortiGates running FortiOS 7.0.x, FortiManager automatically downgrades the 7.0 CLI to 6.4 CLI for FortiGates running FortiOS 6.4.x.

For example, the following policy package is for ADOM 7.0:



You can install the policy package to FortiGate devices in ADOM 7.0 running both FortiOS 6.4.x and FortiOS 7.0.x. In the preview for both devices, you can view what is installed to each device:



ADOM upgrade from 6.4 to 7.0 - 7.0.1

With FortiManager 7.0.1 and later, you can upgrade ADOM version 6.4 to 7.0. This topic describes the recommended ADOM upgrade method. See also [Managing mixed FortiOS versions 6.4 and 7.0 in a single ADOM 7.0.1 on page 112](#).

To upgrade ADOM version 6.4 to 7.0:

1. In ADOM version 6.4, upgrade all FortiGates to FortiOS version 7.0.x.

For example, FortiGates in ADOM version 6.4 are running FortiOS 6.4.x, and the FortiOS version should be upgraded to 7.0.x.

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	Platform	Provisioning Templates	Description
FGT-100	✓ Synchronized	✓ FGT-100_root	FortiGate 6.4.5.build1828 (GA)	FGT-100	FortiGate-VM64		
FortiGate-140E-POE (5)	✓ Synchronized	✓ Synchronized	FortiGate 6.4.5.build1828 (GA)	FortiGate-140E-POE	FortiGate-140E-POE		
root [NAT]	✓ Synchronized	⚠ Never installed			vdmm		
ss [Transparent]	✓ Synchronized	⚠ Never installed			vdmm		
vd-tp [Transparent]	✓ Synchronized	⚠ Never installed			vdmm		
vdmm1 [NAT] (Management)	✓ Synchronized	✓ FortiGate-140E-POE_vdmm1			vdmm		
vdmm2 [NAT]	✓ Synchronized	✓ FortiGate-140E-POE_vdmm2			vdmm		

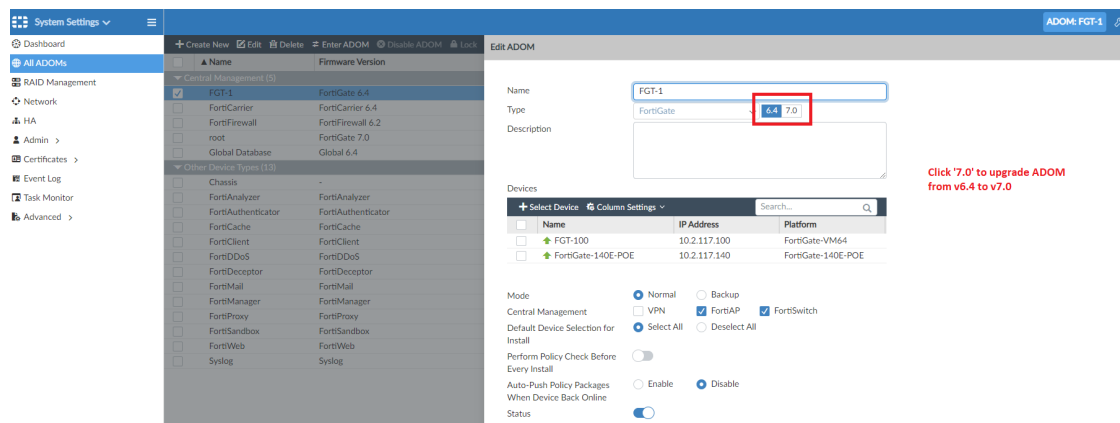
After upgrading FortiOS for all FortiGates in ADOM version 6.4, you see FortiGates are running FortiOS 7.0.1.

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	Platform	Provisioning Templates	Description
FGT-100	✓ Synchronized	✓ FGT-100_root	FortiGate 7.0.1.build1828 (GA)	FGT-100	FortiGate-VM64		
FortiGate-140E-POE (5)	✓ Synchronized	✓ Synchronized	FortiGate 7.0.1.build1828 (GA)	FortiGate-140E-POE	FortiGate-140E-POE		
root [NAT]	✓ Synchronized	⚠ Never installed			vdmm		
ss [Transparent]	✓ Synchronized	⚠ Never installed			vdmm		
vd-tp [Transparent]	✓ Synchronized	⚠ Never installed			vdmm		
vdmm1 [NAT] (Management)	✓ Synchronized	✓ FortiGate-140E-POE_vdmm1			vdmm		
vdmm2 [NAT]	✓ Synchronized	✓ FortiGate-140E-POE_vdmm2			vdmm		

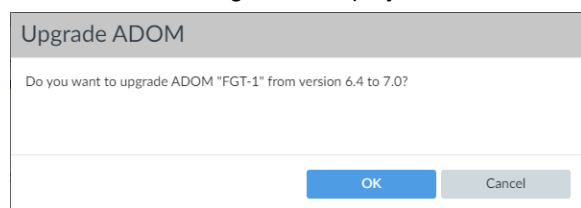
2. Go to **System Settings > All ADOMs**, and from the **More** menu, select **Upgrade**.

Name	Firmware Version	Devices	Comments
FGT-1	FortiGate 6.4	6 Devices >	
FortiCarrier	FortiCarrier 6.4		
FortiFirewall	FortiFirewall 6.2		
Global Database	Global 6.4		

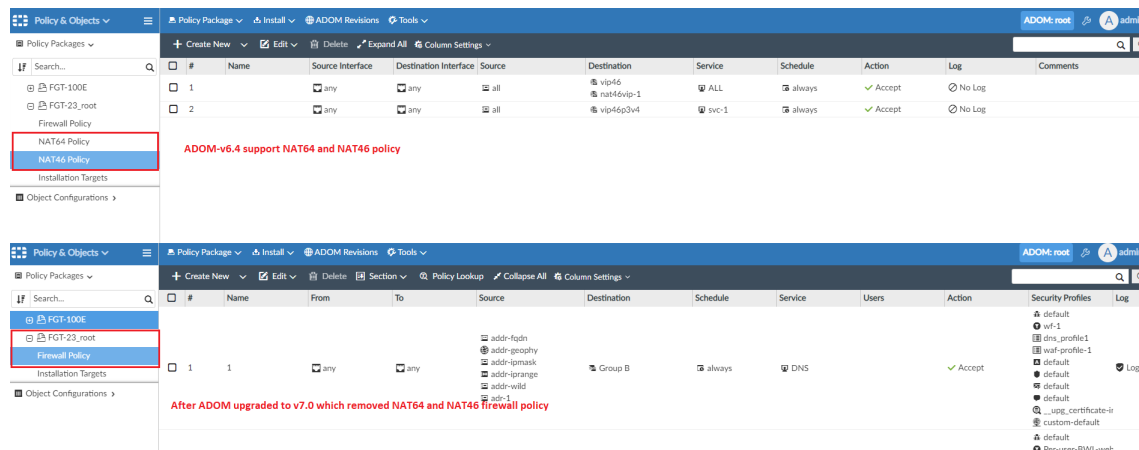
Alternately, you can double-click an ADOM to open it for editing, and click 7.0 to upgrade the ADOM.



A confirmation dialog box is displayed. Click OK to initiate the ADOM upgrade.



The ADOM upgrades from 6.4 to 7.0, and the FortiManager GUI automatically displays features that are available with version 7.0.



For example, all objects in the database for policy and objects are converted to 7.0. You can create a new firewall policy for version 7.0 and install it to FortiGates.

Following is an example of a 7.0 feature available in the firewall policy:

Create New Firewall Policy

Name: NEW-full-ZTNA-policy

ZTNA: Disable Full ZTNA IP/MAC filtering

Incoming Interface: any

Source Internet Service: OFF

IPv4 Source Address: all

Source User: +

Source User Group: +

FSSO Groups: +

ZTNA Server: ZTNA_S1

Service: ALL

Schedule: always

Action: Deny Accept IPSEC

Proxy HTTP(S) Traffic: OFF

Firewall/Network Options

NAT: ☐

Logging Options

Log Traffic: No Log Log Security Events Log All Sessions

☐ Capture Packets

☐ Generate Logs when Session Starts

Advanced

WCCP: ☐

Exempt from Captive Portal: ☐

Comments:

Object Selector

Search...

FIREWALL ACCESS-PROXY (1)

ZTNA_S1

From the *Installation* wizard, you can preview the changes before you install them to FortiGates:

Install Preview of FGT-100

```

30: config firewall address
31:   edit "all"
32:     set uuid 26c07b02-f482-51eb-2c70-b8ff9b0676d5
33:   next
34: end
35: config webfilter ftgd-local-rating
36:   edit "youtube.com"
37:     set rating "140"
38:   next
39: end
40: config firewall policy
41:   edit 4
42:     set name "NEW-full-ZTNA-policy"
43:     set uuid e42c380a-f489-51eb-217a-a18ad7298a57
44:     set action accept
45:     set inspection-mode proxy
46:     set srcintf "any"
47:     set dstintf "any"
48:     set srcaddr "all"
49:     set dstaddr "ZTNA_S1"
50:     set schedule "always"
51:     set service "ALL"
52:     set logtraffic all
53:   next
54: end

```

[Download](#) [Close](#)

Management Extensions

This section lists the other new features added to FortiManager for management extensions:

- CPU and RAM maximum values for Management Extension Applications can be configured in CLI on page 117
- New management extension - FortiSOAR on page 117
- New management extension - FortiAIOps 7.0.1 on page 120
- New management extension - Universal Connector 7.0.1 on page 123

CPU and RAM maximum values for Management Extension Applications can be configured in CLI

You can allocate up to 50% (between 10% and 50 %) of the total FortiManager resource to management extension applications. This ensures that there are no performance issues in the host FortiManager.

To limit CPU and RAM for management extensions:

1. In the FortiManager CLI, use the following commands:

```
config system docker
    set cpu <integer> #use this variable to set the maximum % of CPU usage.
    set mem <integer> #use this variable to set the maximum % of RAM usage.
end
```

For details about the CLI commands and variables used here, see the *FortiManager 7.0.0 CLI Reference* on the [Fortinet Docs Library](#).



- The CLI commands allow you to set the resource limit globally for all management extensions.
- If management extensions reach the limit of allocated FortiManager resource, a warning appears in the *Alert Message Console* widget in *System Settings > Dashboard*.

New management extension - FortiSOAR

This feature adds the FortiSOAR application as a management extension application (MEA). FortiSOAR is an enterprise-built security orchestration and security automation workbench that empowers security operation teams.

By default, FortiSOAR MEA is disabled. You can enable FortiSOAR MEA by using the GUI or the CLI.

There are minimum system resources recommended for FortiManager when using FortiSOAR MEA. See the FortiManager Release Notes for additional information.

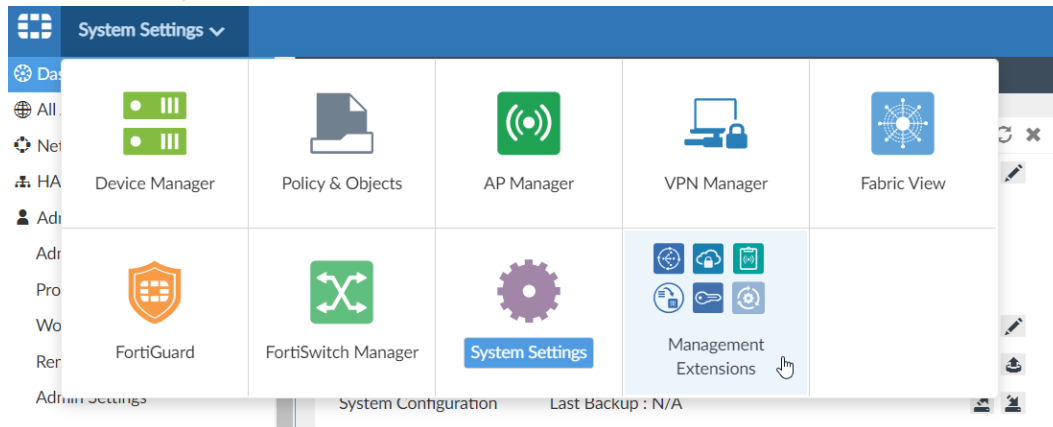
The following CLI commands are available for FortiSOAR MEA:

- `config system docker`
- `diagnose docker status`

- `diagnose docker upgrade fortisoar`

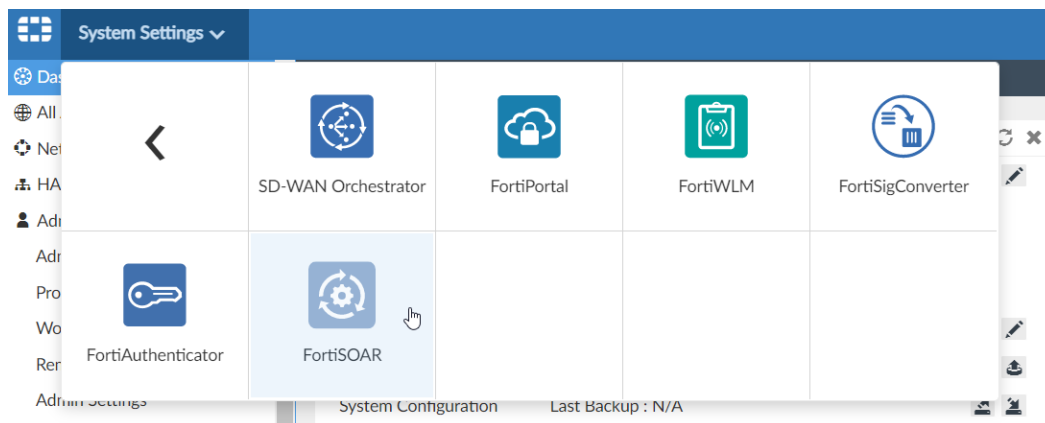
To enable FortiSOAR MEA by using the GUI:

1. Ensure you are logged in to FortiManager by using an administrator account that is assigned a *Super_User* profile.
2. Go to the *Management Extensions* tile.



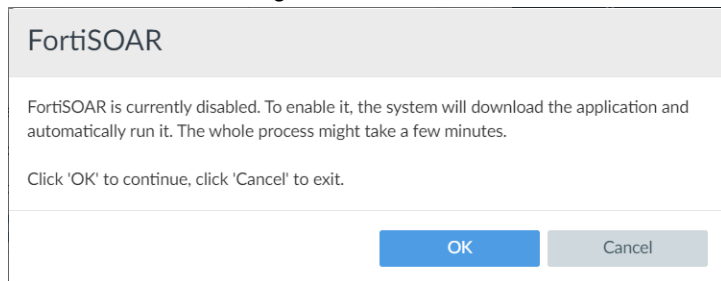
The management extension application options are displayed.

3. Click *FortiSOAR*.



A confirmation dialog box is displayed.

4. In the confirmation dialog box, click *OK*.

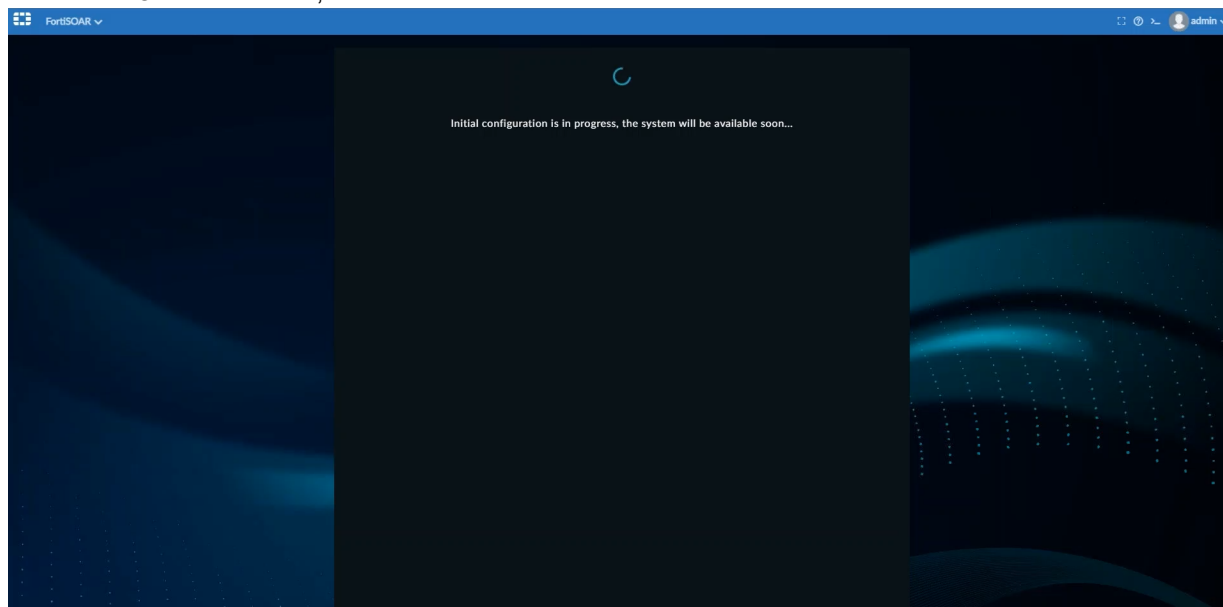


FortiSOAR MEA is downloaded from the Fortinet registry (registry.fortinet.com).

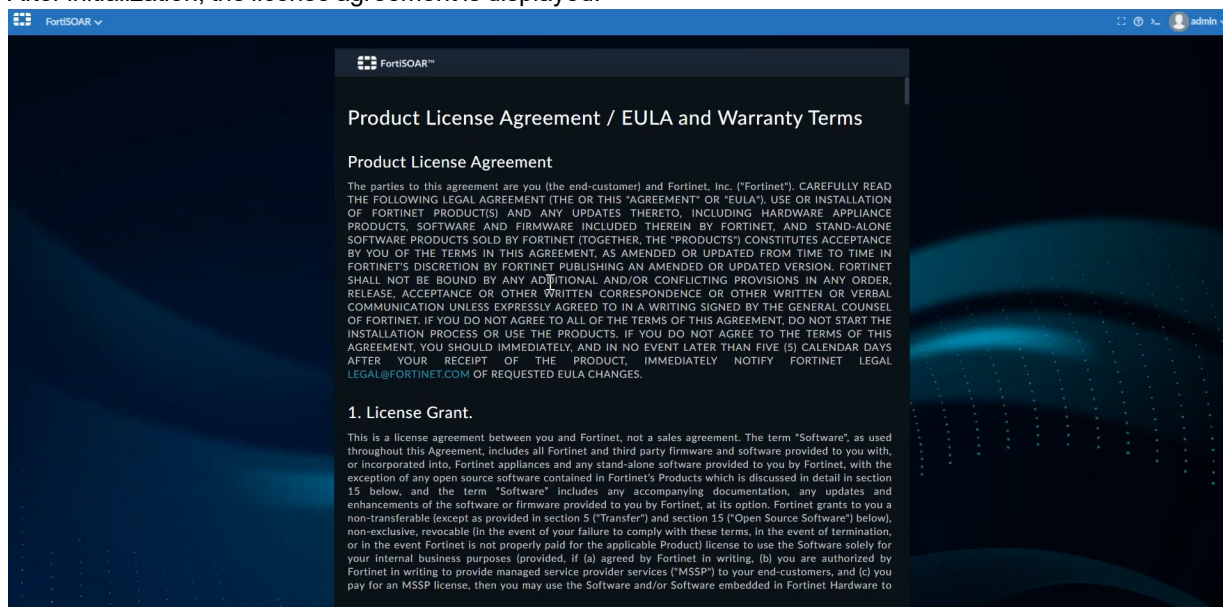
A progress bar displays under the FortiSOAR tile.



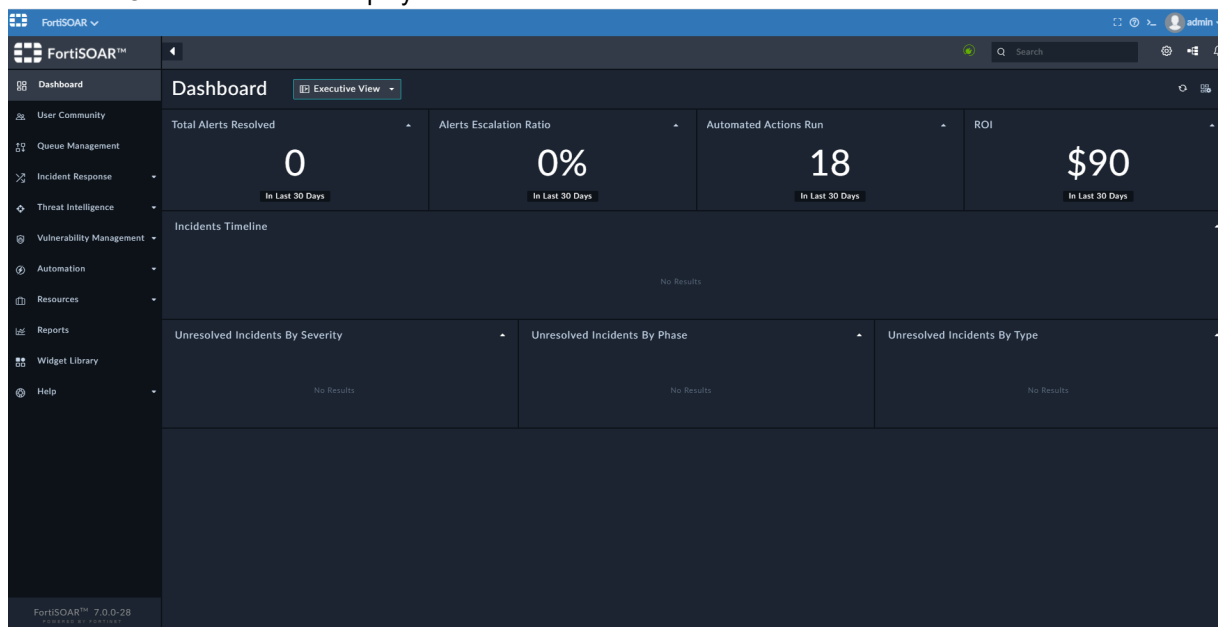
After FortiSOAR downloads, it initializes.



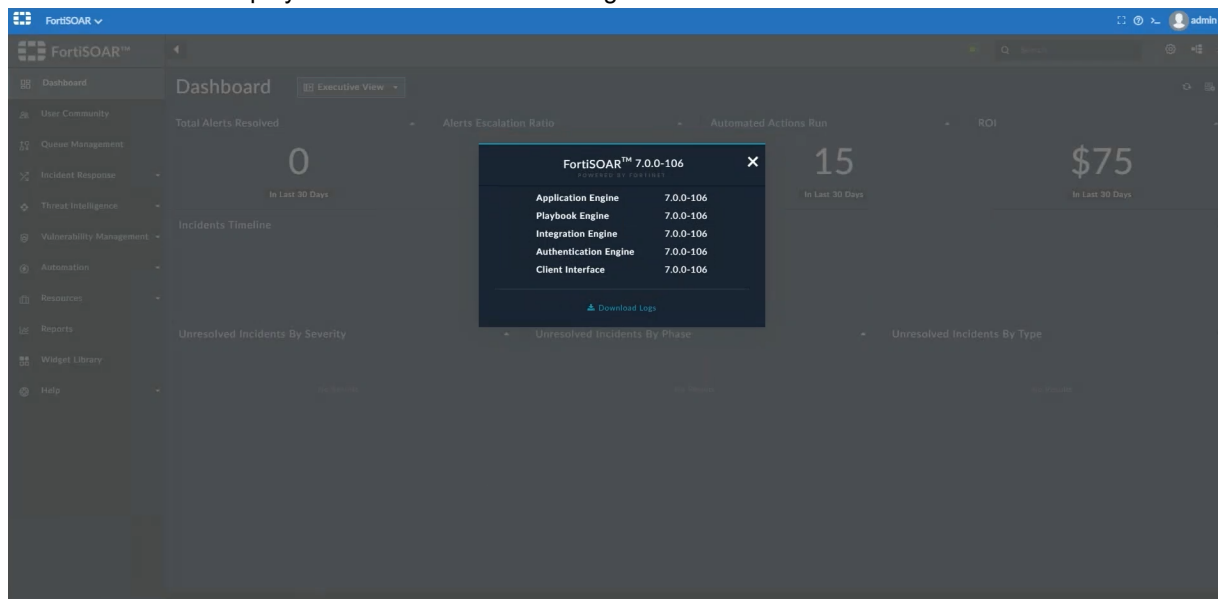
After initialization, the license agreement is displayed.



5. Read the license agreement, and click *Agree*.
6. Log in to FortiSOAR by using your FortiManager login.
The FortiSOAR dashboard is displayed.



The version and build information for FortiSOAR can be found on the bottom-left corner of the Dashboard. Clicking on this information displays the version and build dialog.



New management extension - FortiAIOPS - 7.0.1

This feature adds the FortiAIOPS application as a management extension application (MEA). FortiAIOPS helps network administrators monitor, identify, and troubleshoot wired and wireless networks or devices and connected users or

clients.

It analyzes data based on the SLAs configured on the *Configuration* tab, and displays the data on the *Monitor* tab. Data is retained two days for analyzing.

FortiAIops MEA includes a default license that supports one FortiGate device. If you want to analyze data from two or more FortiGate devices, you can purchase a license, and use the *Devices* tab to upload the license to the *Licenses* section.

By default, FortiAIops MEA is disabled. You can enable FortiAIops MEA by using the GUI or the CLI.

For information about minimum system resources recommended for FortiManager when using FortiAIops MEA, see the [FortiManager Release Notes](#).

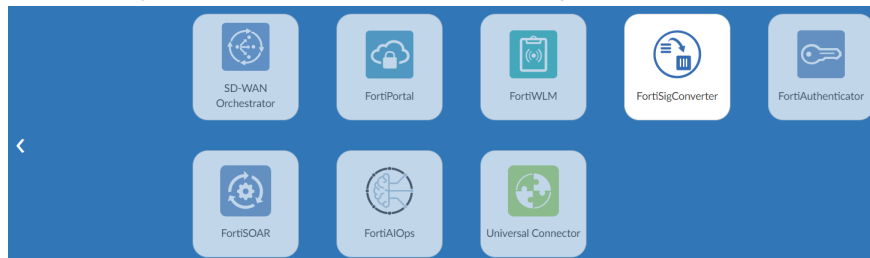
For information about using FortiAIops MEA, see the [FortiAIops 1.0.0 User Guide](#).

The following CLI commands are available for FortiAIops MEA:

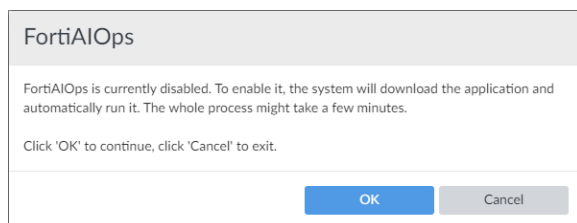
- `config system docker`
- `diagnose docker status`
- `diagnose docker upgrade fortiaios`

To enable FortiAIops MEA by using the GUI:

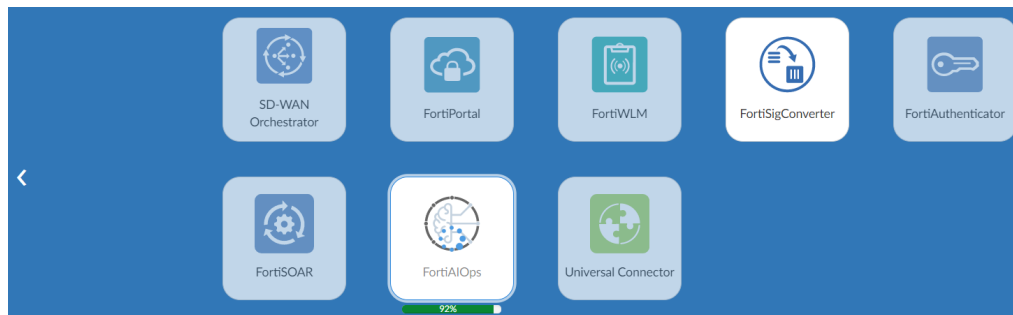
1. Ensure you are logged in to FortiManager by using an administrator account that is assigned a *Super_User* profile.
2. Go to *Management Extensions*, and click *FortiAIops*.



A confirmation dialog box is displayed.



3. In the confirmation dialog box, click *OK*.
As long as FortiManager has access to the Internet, FortiAIops MEA is downloaded from the Fortinet registry (registry.fortinet.com). A progress bar displays under the FortiAIops tile.

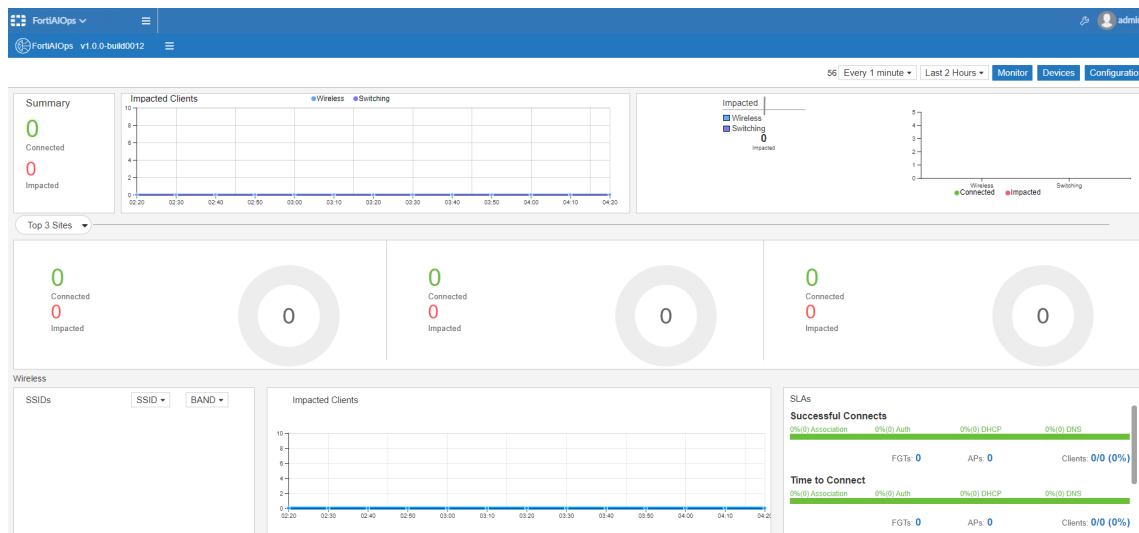


After FortiAIOPS is downloaded, the *FortiAIOPS* tile is available.



4. Click *FortiAIOPS*.

The *Monitor* tab is displayed by default.



5. Click the *Devices* tab to access information about licenses and devices.

FortiManager v1.0.0-build50012

51 | Every 1 minute | Monitor | **Devices** | Configuration

LICENSES

Upload License | Search

System ID: 10fdca7b686d9aced70bb8274d9627b

Feature	Start Date	Expiry Date	Number of Licenses	File Name
No results				

DEVICE(S)

Add | Edit | Delete | Search

FGT ID	FGT Serial	HostName	IP Address	Model	Software Version	Port	Availability State	Management State	Administrative State
1	FGVN08TM21001806	FGVN08TM21001806	10.2.135.63	FGVN08	v7.0.0	443	Online	Active	Managed

6. Click the *Configuration* tab to configure SLA.

FortiManager v1.0.0-build50012

Monitor | Devices | **Configuration**

SLA CONFIGURATIONS

Time To Connect

Association Time(Milli Seconds) 300

Authentication Time(Milli Seconds) 300

DHCP Time(Milli Seconds) 300

DNS Time(Milli Seconds) 300

AP Health

CPU 60

Memory 60

Temperature(°F) 64.4

Switch Health

CPU 60

Memory 60

Temperature(°F) 64.4

OK Cancel

New management extension - Universal Connector - 7.0.1

This feature adds the Universal Connector application as a management extension application (MEA). You can use Universal Connector to create fabric connectors to external applications, such as Guardicore Centra Security Platform.

Universal Connector does not require a license. It is free to use.

By default, Universal Connector is disabled. You can enable Universal Connector by using the GUI or the CLI.

For information about minimum system resources recommended for FortiManager when using Universal Connector, see the [FortiManager Release Notes](#).

For information about using Universal Connector, see the [Universal Connector Administration Guide](#).

The following CLI commands are available for Universal Connector:

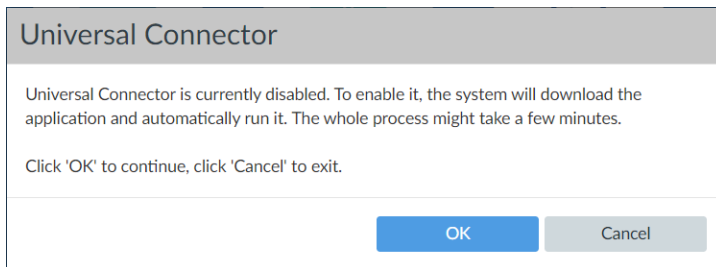
- `config system docker`
- `diagnose docker status`
- `diagnose docker upgrade universalconnector`

To enable Universal Connector MEA by using the GUI:

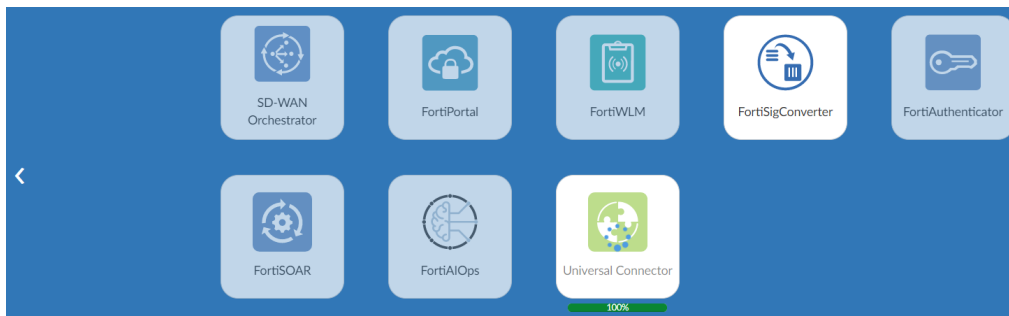
1. Ensure you are logged in to FortiManager by using an administrator account that is assigned a *Super_User* profile.
2. Go to *Management Extensions*, and click *Universal Connector*.



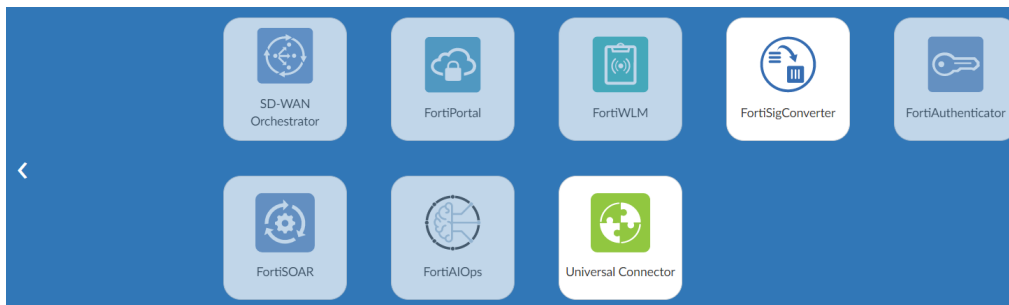
A confirmation dialog box is displayed.



3. In the confirmation dialog box, click *OK*.
As long as FortiManager has access to the Internet, Universal Connector MEA is downloaded from the Fortinet registry (registry.fortinet.com). A progress bar displays under the Universal Connector tile.



After Universal Connector is downloaded, the *Universal Connector* tile is available.



4. Click *Universal Connector*.
Universal Connector opens.



5. Create a connector to Guardicore Centra. For details, see the [Universal Connector Administration Guide](#).

Other

This section lists other new features added to FortiManager:

- [FortiManager Setup wizard on page 126](#)
- [FortiManager VM licenses on page 131](#)
- [GUI reorganization on page 138](#)
- [FortiManager VM supports Amazon EC2 IMDS version 2 on page 146](#)
- [Country list for direct registration 7.0.1 on page 146](#)
- [Event log easier to read 7.0.1 on page 146](#)
- [Local FortiGuard Distribution Server enhancements 7.0.1 on page 147](#)
- [NSX-T service template with VDOM support 7.0.1 on page 151](#)

FortiManager Setup wizard

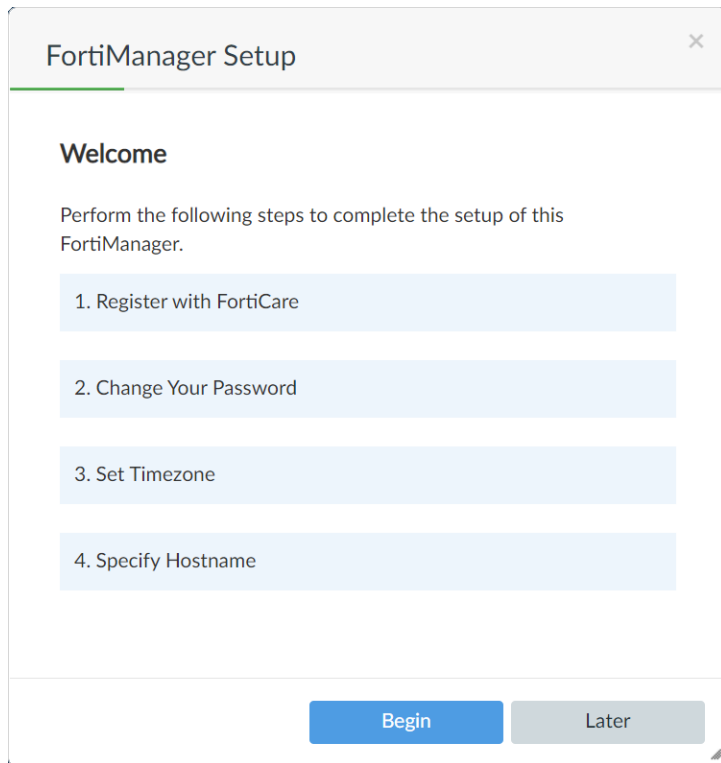
The FortiManager Setup wizard lets you register with FortiCare as well as perform the following actions:

- Registering with FortiCare
- Changing your password
- Setting the time zone
- Specifying a hostname

When an action is complete, a green checkmark displays it in the wizard, and the wizard no longer displays after you log in to FortiManager.

To use the FortiManager Setup wizard:

1. Log in to FortiManager.
The *FortiManager Setup* dialog box is displayed.



The image shows the 'FortiManager Setup' window with a 'Welcome' section. It lists four steps: 1. Register with FortiCare, 2. Change Your Password, 3. Set Timezone, and 4. Specify Hostname. At the bottom, there are 'Begin' and 'Later' buttons.

FortiManager Setup

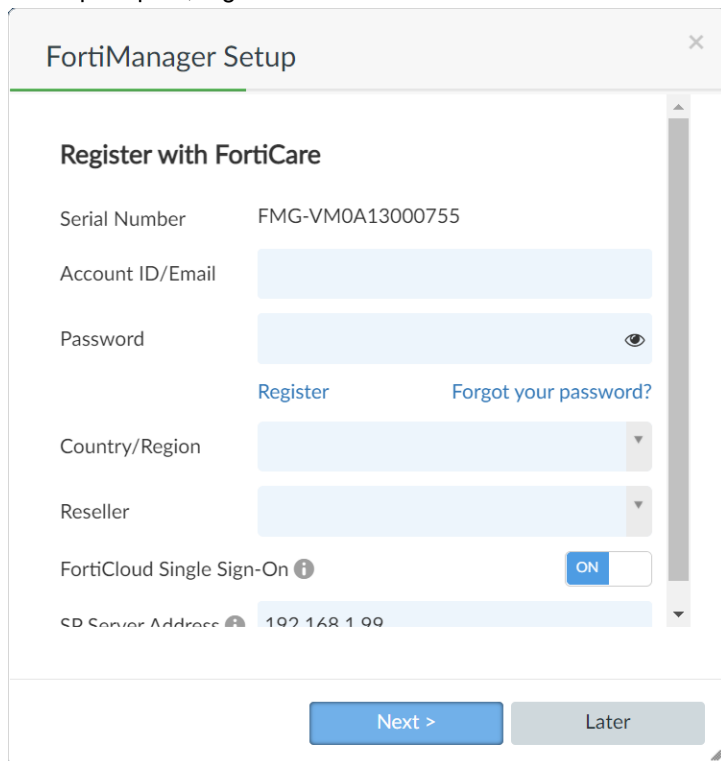
Welcome

Perform the following steps to complete the setup of this FortiManager.

1. Register with FortiCare
2. Change Your Password
3. Set Timezone
4. Specify Hostname

Begin **Later**

2. Click *Begin* to start the setup process now.
Alternately, click *Later* to postpone the setup tasks.
3. When prompted, register with FortiCare.




The image shows the 'FortiManager Setup' window with the 'Register with FortiCare' section. It includes fields for Serial Number, Account ID/Email, Password, Country/Region, Reseller, and FortiCloud Single Sign-On. There are also links for 'Register' and 'Forgot your password?'. At the bottom, there are 'Next >' and 'Later' buttons.

FortiManager Setup

Register with FortiCare

Serial Number: FMG-VM0A13000755


Account ID/Email:


Password: 

[Register](#) [Forgot your password?](#)

Country/Region:

Reseller:

FortiCloud Single Sign-On  ☒ **ON**

SD Server Address 

Next > **Later**

- a. In the *Account ID/Email* box, type your FortiCare account ID or email.
If you do not yet have a FortiCare account, click *Register* to create a new account.

- b. In the *Password* box, type your FortiCare password.
If you have forgotten your FortiCare password, click *Forgot your password* to proceed through the password recovery process.
 - c. In the *Country/Region* box, select your country or region from the dropdown.
 - d. In the *Reseller* box, select your reseller from the dropdown.
 - e. Set the *FortiCloud Single Sign-On* toggle to the *ON* or *OFF* position to enable or disable FortiCloud SSO sign on.
When enabled, you must also enter the *SP Server Address*.
 - f. Click *Next*.
4. When prompted, change your password.

FortiManager Setup

Change Your Password

This account is using the default password. It is strongly recommended that you change your password.

Old Password

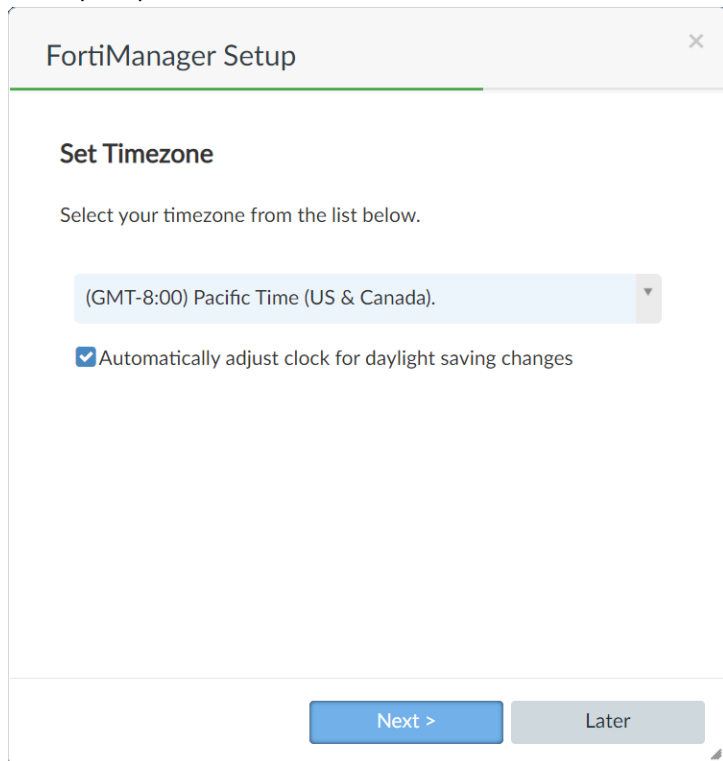
New Password

Confirm Password

Next > Later

- a. In the *Old Password* box, type the old password.
- b. In the *New Password* box, type the new password.
- c. In the *Confirm Password* box, type the new password again.
- d. Click *Next*.

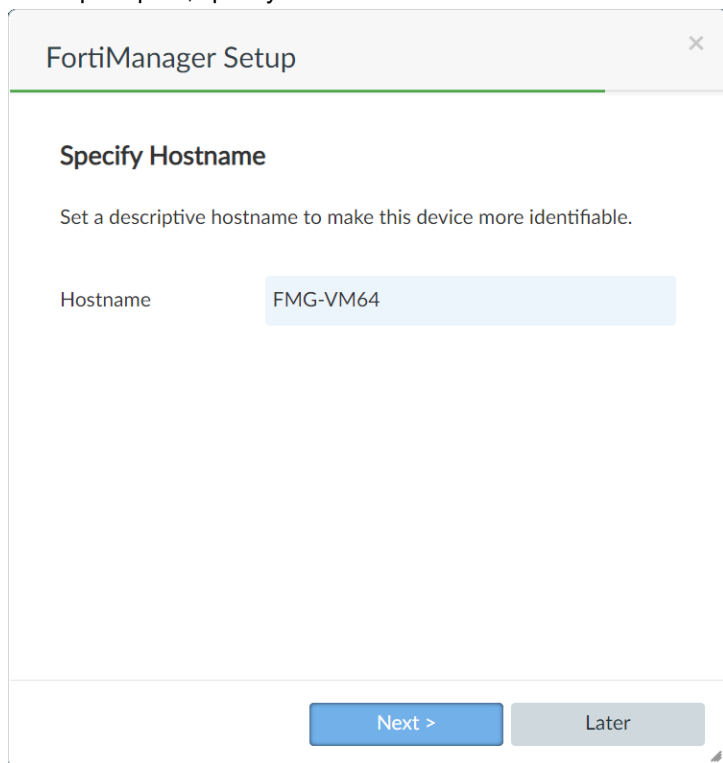
5. When prompted, set the time zone.



The image shows a 'FortiManager Setup' dialog box with a close button (X) in the top right corner. The title bar is 'FortiManager Setup'. The main content area is titled 'Set Timezone'. Below the title, it says 'Select your timezone from the list below.' There is a dropdown menu showing '(GMT-8:00) Pacific Time (US & Canada)'. Below the dropdown is a checkbox labeled 'Automatically adjust clock for daylight saving changes' which is checked. At the bottom of the dialog, there are two buttons: 'Next >' (blue) and 'Later' (grey).

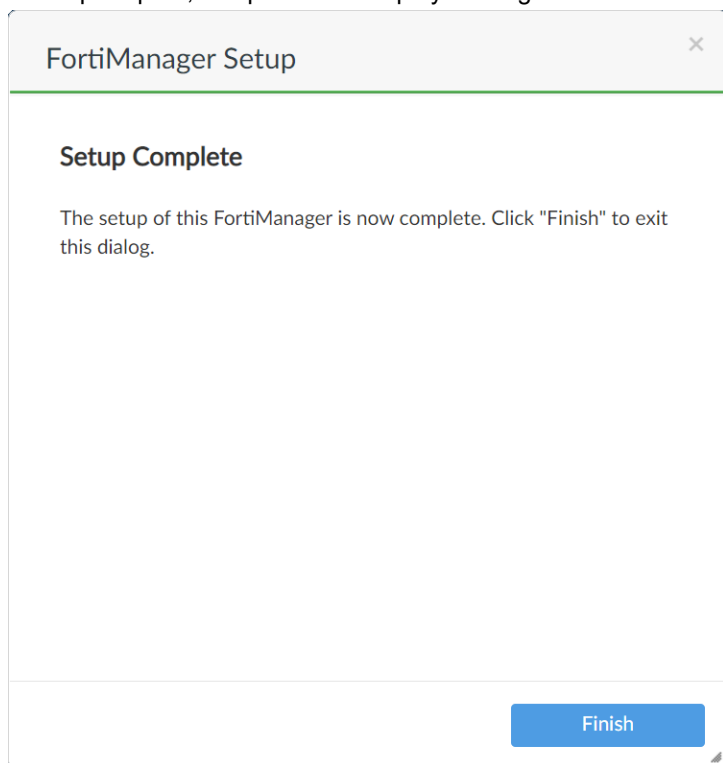
- a. From the list, select the time zone.
- b. (Optional) Clear the *Automatically adjust clock for daylight savings changes* checkbox if desired. By default FortiManager is configured to automatically adjust closed for daylight savings.
- c. Click *Next*.

6. When prompted, specify the hostname.



The image shows a 'FortiManager Setup' dialog box with a title bar containing a close button. The main content area is titled 'Specify Hostname' and includes the instruction 'Set a descriptive hostname to make this device more identifiable.' Below this, there is a 'Hostname' label followed by a text input field containing 'FMG-VM64'. At the bottom right, there are two buttons: 'Next >' (highlighted in blue) and 'Later' (disabled, greyed out).

- a. In the *Hostname* box, type a hostname.
b. Click *Next*.
7. When prompted, complete the setup by clicking *Finish*.



The image shows a 'FortiManager Setup' dialog box with a title bar containing a close button. The main content area is titled 'Setup Complete' and includes the instruction 'The setup of this FortiManager is now complete. Click "Finish" to exit this dialog.' At the bottom right, there is a single blue button labeled 'Finish'.

You are logged in to FortiManager.

FortiManager VM licenses

For FortiManager virtual machines (VMs), you can use the FortiManager GUI to:

- Request and activate a trial license
- Activate a perpetual or VM-S license
- Activate an add-on perpetual or VM-S license

FortiManager must be able to access the Internet to communicate with FortiCloud to complete the licensing process.

The licensing process requires you to log in to FortiCloud. If you do not have a FortiCloud account, you can create one to complete the licensing process.

This topic contains the following sections:

- [Requesting and activating a trial license on page 131](#)
- [Activating a new license on page 134](#)
- [Activating an add-on license on page 136](#)

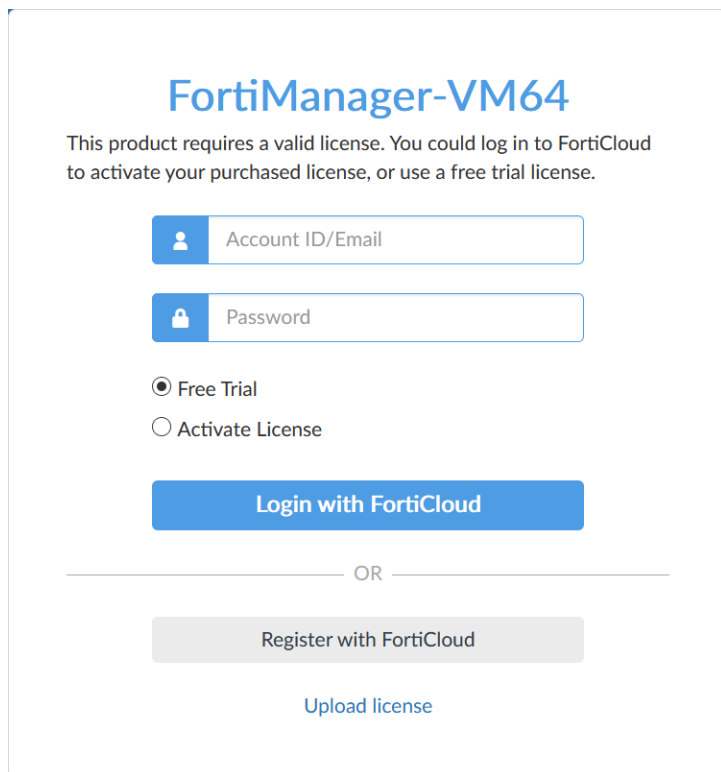
Some of the screen shots in the following examples are for FortiManager, but the process applies to both FortiManager and FortiAnalyzer.

Requesting and activating a trial license

You can use the FortiManager GUI to request and activate a trial license for a FortiManager VM.

To request and activate a trial license:

1. In a browser, access the IP address for the FortiManager GUI.
The login dialog box is displayed.



The image shows the FortiManager-VM64 login and registration interface. At the top, the title "FortiManager-VM64" is displayed in blue. Below the title, a message states: "This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license." The interface includes two input fields: "Account ID/Email" and "Password", each with a corresponding icon (a person and a lock respectively). Below these fields are two radio buttons: "Free Trial" (selected) and "Activate License". A blue button labeled "Login with FortiCloud" is positioned below the radio buttons. A horizontal line with the word "OR" in the center separates this from a gray button labeled "Register with FortiCloud". At the bottom, there is a blue link labeled "Upload license".

2. Select *Free Trial*, and click *Login with FortiCloud*.
If you do not have a FortiCloud account, click *Register with FortiCloud* to create one.
The *Free Trial License Agreement* is displayed.

Free Trial License Agreement



FortiAnalyzer-VM/FortiManager-VM Free Limited License Agreement

TERMS AND CONDITIONS

THESE TERMS AND CONDITIONS APPLY BETWEEN THE ENTITY SET FORTH BELOW (THE "CUSTOMER") AND FORTINET, WHERE BOTH PARTIES CONSENT TO BE BOUND BY THESE TERMS AND CONDITIONS UNDER THIS FREE LIMITED LICENSE AGREEMENT (THE "AGREEMENT"). IF YOU DO NOT AGREE TO THE TERMS, YOU SHOULD NOT ACCEPT THE AGREEMENT AND SHOULD CONTACT LEGAL@FORTINET.COM TO REQUEST CHANGES TO THE AGREEMENT

1) FREE LIMITED LICENSE AGREEMENT.

This Agreement is made for the purpose of testing and evaluating Fortinet's FortiAnalyzer and FortiManager Virtual Machine which have limited features as compared to the full version (hereinafter the "Products") for their potential purchase. Although the Products will have limited features (as detailed below), they will allow Customer to determine if they perform to specifications and expectations.

2) PERMITTED USES AND RESTRICTIONS FOR THE LICENSE.

Fortinet grants Customer a nonexclusive, and nontransferable, limited license to use the Products for testing and evaluation (either by Customer or a third party evaluator). Customers will be provided with 1 limited free trial of the Products with their FortiCare account. The Products will include a maximum of 1 GB/day logs, 3 devices, 2 ADOMs, and do not include services or support, such as FortiCare (support and maintenance) or FortiGuard (subscription services). Customer may use the Products for management and analytics of data generated by other Fortinet products. The trial license does not come with any obligation or promise by Fortinet to provide FortiCare (support and maintenance) or FortiGuard (subscription services). Customer's access and use of the Products are subject to the limitations of their respective trial versions and are subject to all of Fortinet's applicable the terms and conditions, including Fortinet's then current End User License Agreement ("EULA") which can be found at: <http://www.fortinet.com/doc/legal/EULA.pdf> and Fortinet Service Terms and Conditions ("Terms of Service") which can be found at <https://www.fortinet.com/content/dam/fortinet>

☒ I have read and accept the terms in the License Agreement.

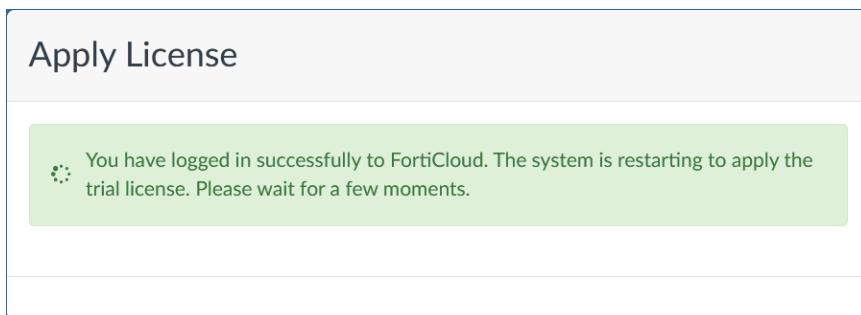
Accept

Cancel

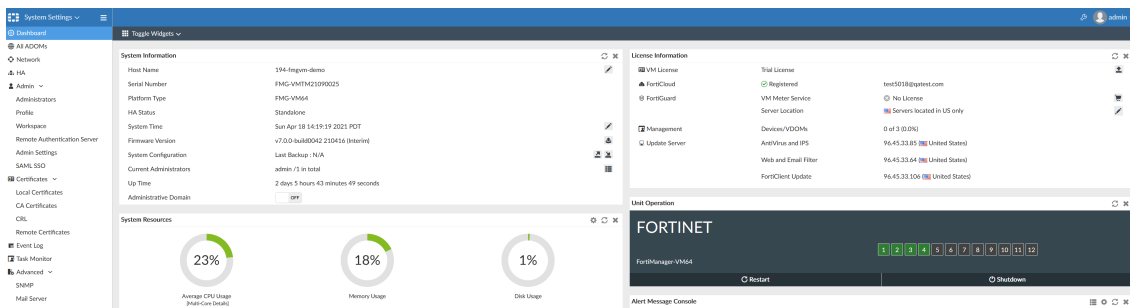
3. Accept the license agreement:

- a. Read the license agreement.
- b. Select the *I have read and accept the terms in the License Agreement* checkbox.
- c. Click *Accept*.

The license is applied, and you are logged in to FortiManager.



4. Go to **System Settings > Dashboard > License Information** widget. The **VM License** option displays **Trial License**.



Activating a new license


You can use the FortiManager GUI to activate a new license for virtual machines. Licenses for VM-S subscriptions and perpetual subscriptions are supported.

To activate a new license:


1. In a browser, access the IP address for the FortiManager GUI. The login dialog box is displayed.

FortiManager-VM64

This product requires a valid license. You could log in to FortiCloud to activate your purchased license, or use a free trial license.



test5018@qatest.com



●●●●●●●●

☐ Free Trial

☒ Activate License

FGMKW-1FCWA-QCEN6-VK0QK-Z260QF

1.1.1.1

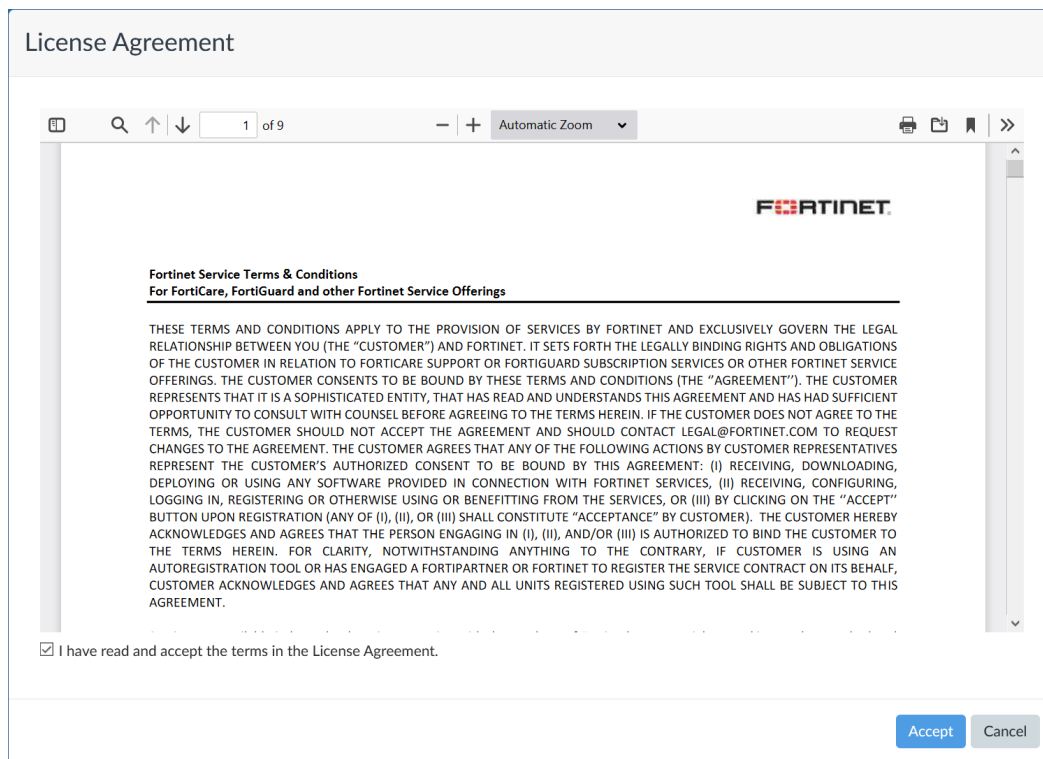
Login with FortiCloud

OR

Register with FortiCloud

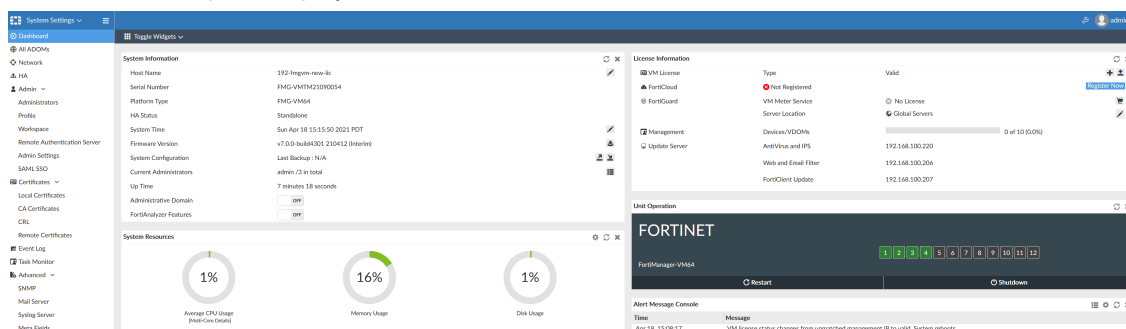
[Upload license](#)

2. Select *Activate License*, enter your license key, and click *Login with FortiCloud*. The *License Agreement* is displayed.



3. Accept the license agreement:
 - a. Read the license agreement.
 - b. Select the *I have read and accept the terms in the License Agreement* checkbox.
 - c. Click **Accept**.

The license is applied, and you are logged in to FortiManager.
4. Go to **System Settings > Dashboard > License Information** widget.
The **VM License** option displays **Valid**.



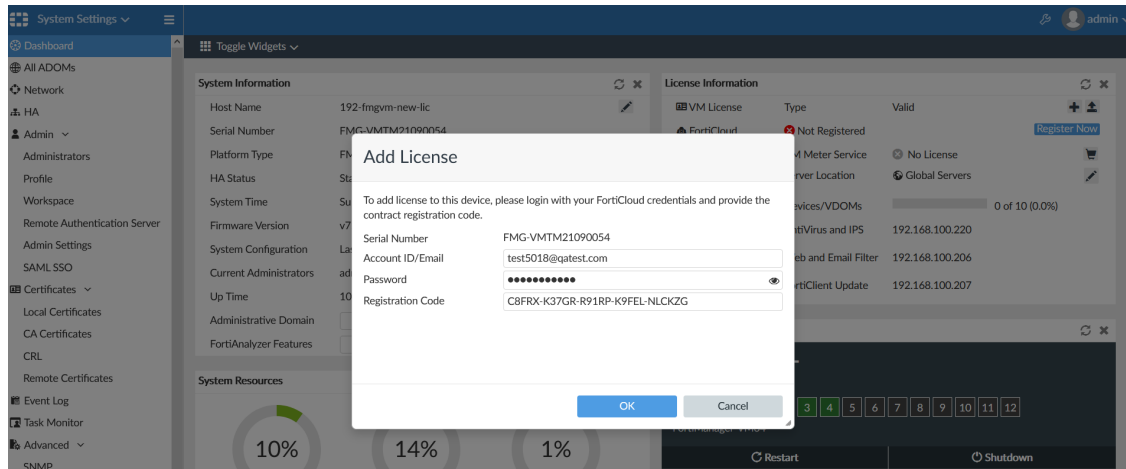
Activating an add-on license

You can use the FortiManager GUI to activate an add-on license for a VM-S subscription or a perpetual subscription.

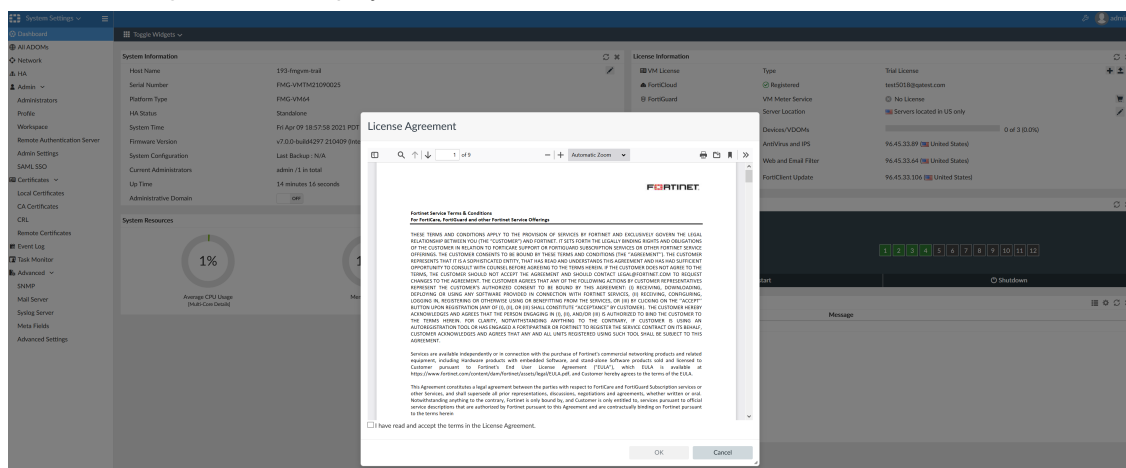
In the following example, the FortiManager VM has a base license, and you want to apply an add-on perpetual license named **1000UG**.

To activate an add-on license:

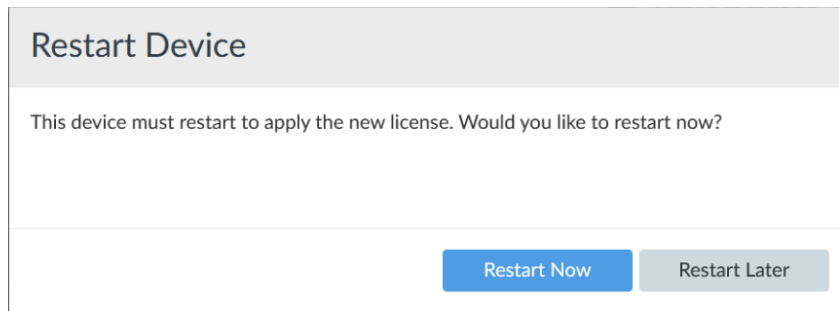
1. Log in to FortiManager, and go to *System Settings > Dashboard*.
2. In the *License Information* widget, beside the *VM License* option, click the *Add License* button. The *Add License* dialog box is displayed.



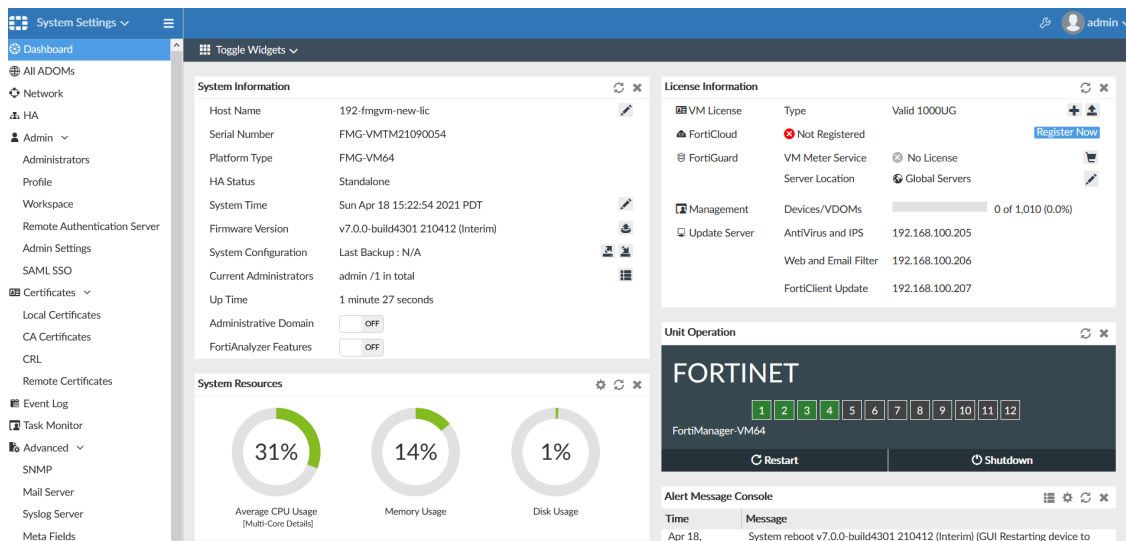
3. Complete the following options, and click **OK**:
 - a. In the *Account ID/Email* box, type the email for your FortiCloud account.
 - b. In the *Password* box, type the password for your FortiCloud account.
 - c. In the *Registration Code* box, enter the contract registration code for the add-on license.
- The *License Agreement* is displayed.



4. Accept the license agreement:
 - a. Read the license agreement.
 - b. Select the *I have read and accept the terms in the License Agreement* checkbox.
 - c. Click **OK**.
- The *Restart Device* dialog box is displayed.



5. Click *Restart Now* to apply the license.
FortiManager restarts, and the license is applied.
6. Go to *System Settings > Dashboard > License Information* widget.
The *VM License* option displays *Valid 1000UG*.



GUI reorganization

The GUI for Per-Device Management view has been reorganized to align with the GUI in FortiOS.

The GUI in the following modules have been reorganized:

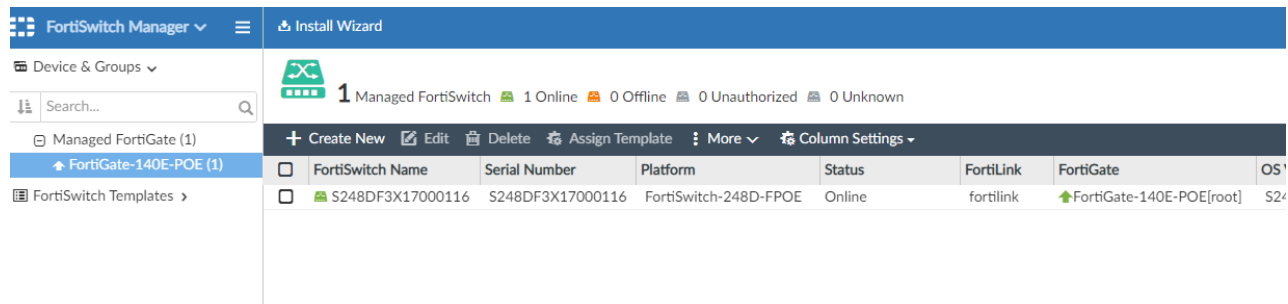
- Device Manager
- AP Manager
- FortiSwitch Manager
- Extender Manager
- VPN Manager

Device Manager

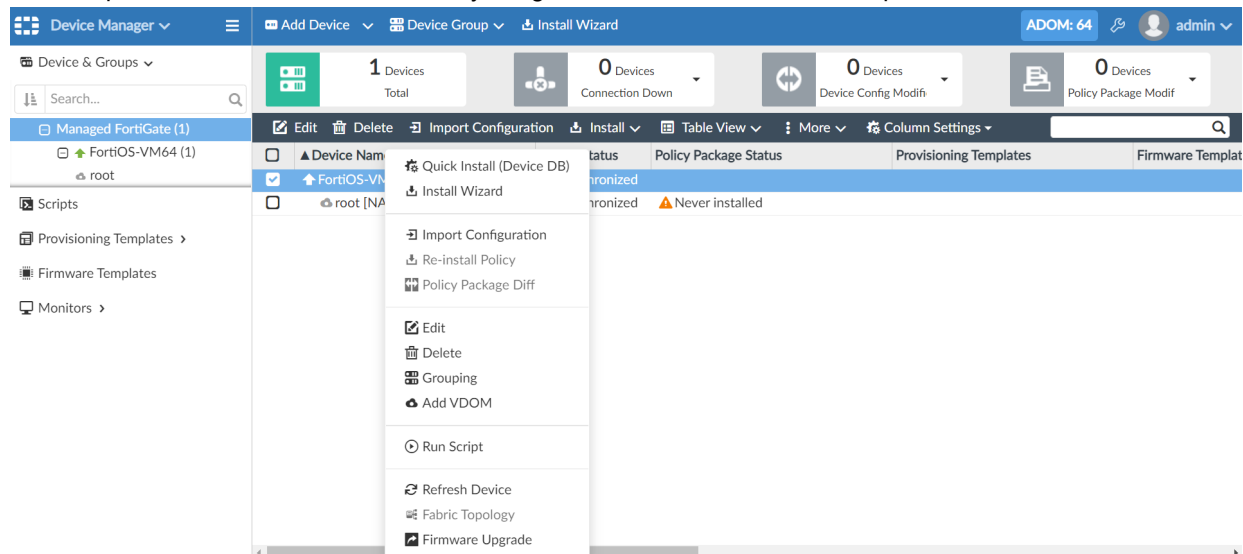
To view the GUI changes in Device Manager:

1. Go to *System Settings > Advanced Settings*.
2. Ensure *Display Policy & Objects in Classic Dual Pane* is disabled.
3. Go to *Device Manager*.
4. In the tree menu, right-click a managed FortiGate device.

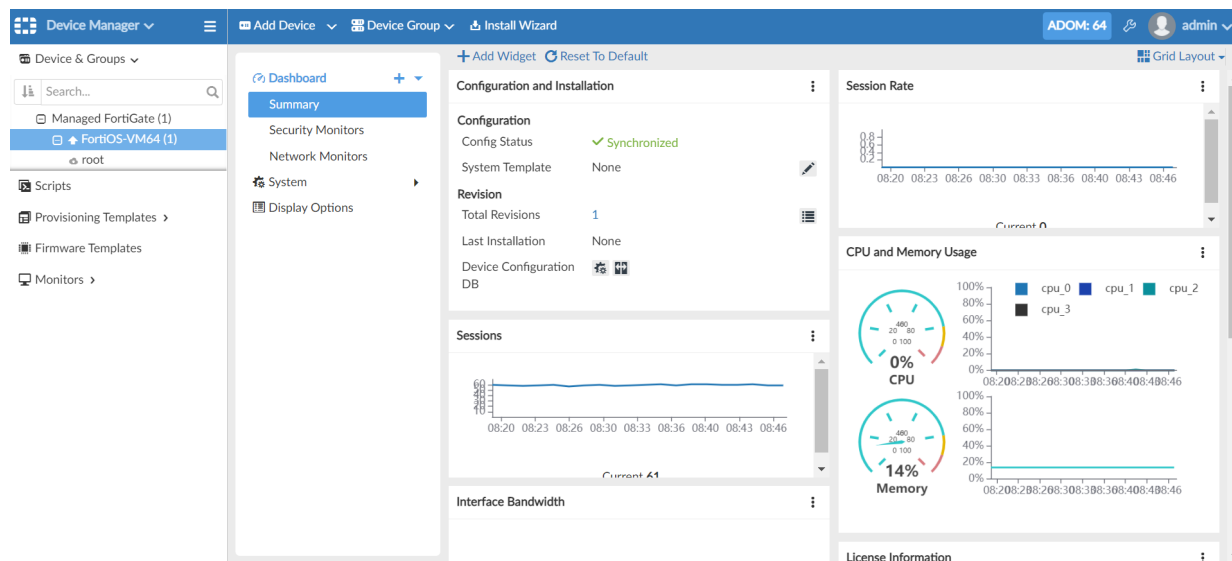
The available options mirror the options in the context menu for the device table, including *Import Policy*, *Re-Install Policy*, *Policy Package Diff*, *Edit*, *Delete*, *Groupings*, *Add VDOM*, *Run Script* and *Firmware Upgrade*.



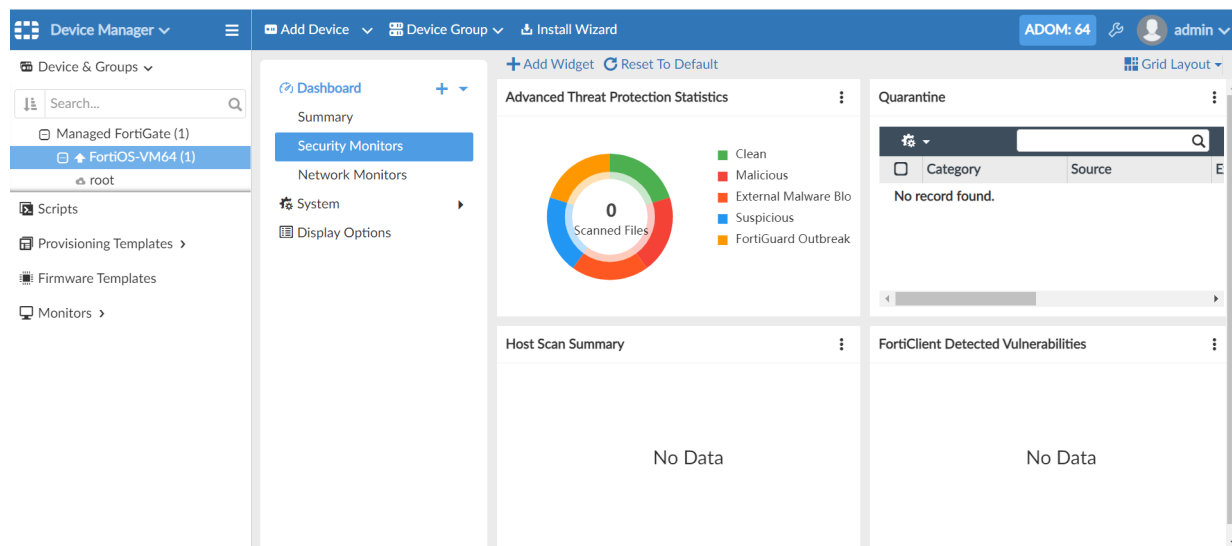
These options are also available in when you right-click a device in the content pane.



5. Double-click a FortiGate. The *Dashboard* sub menu opens.
The *Resources* tab and *Resources* widgets have been merged into the *Summary* tab.



The *Security Monitors* tab was also added to the dashboard.



AP Manager

To view the GUI changes in AP Manager:

1. Go to *AP Manager*. The *Management Mode* indicator has been removed from the banner. In both *Central Management* and *Per Device Management*, the *WiFi Profiles* have been renamed *WiFi Templates* and were moved to the tree menu.

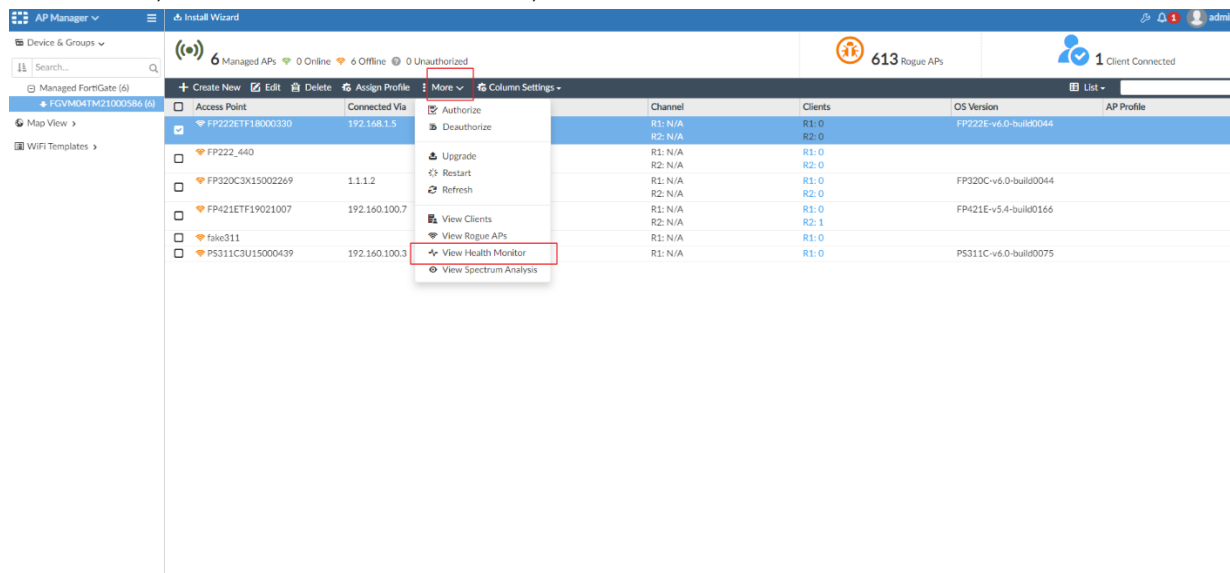
Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
FP222ET18000330	192.168.1.5	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	R1: 1 R2: 48	R1: 0 R2: 0	FP222E-v6.0-build0044	FAP222E-default
FP222_440		R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	R1: 0 R2: 0	R1: 0 R2: 0		FAP222E-default
FP320C3X15002269	1.1.1.2	R1: All Tunnel Mode SSIDs R2: All Tunnel Mode SSIDs	R1: 11 R2: 60	R1: 0 R2: 0	FP320C-v6.0-build0044	FAP320C-default
FP421ET19021007	192.160.100.7	R1: None R2: ssid	R1: 0 R2: 149	R1: 0 R2: 1	FP421E-v5.4-build0166	FAP421E-default
fake311		R1: All Tunnel Mode SSIDs	R1: 0	R1: 0		FAP5311C-default
PSS311C3U15000439	192.160.100.3	R1: All Tunnel Mode SSIDs	R1: 149	R1: 0	PS311C-v6.0-build0075	FAP5311C-default

2. View the Client and Health monitors.

- Right-click a device in the content pane and select *View Clients* to view the *Clients* monitor.

Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
FP222ET18000330	192.168.1.5	R1: N/A R2: N/A	R1: N/A R2: N/A	R1: 0 R2: 0	FP222E-v6.0-build0044	
FP222_440		R1: N/A R2: N/A	R1: N/A R2: N/A	R1: 0 R2: 0		
FP320C3X15002269	1.1.1.2	R1: N/A R2: N/A	R1: N/A R2: N/A	R1: 0 R2: 0	FP320C-v6.0-build0044	
FP421ET19021007	192.160.100.7	R1: N/A R2: N/A	R1: N/A R2: N/A	R1: 0 R2: 1	FP421E-v5.4-build0166	
fake311		R1: N/A	R1: N/A	R1: 0		
PSS311C3U15000439	192.160.100.3	R1: N/A	R1: N/A	R1: 0	PS311C-v6.0-build0075	

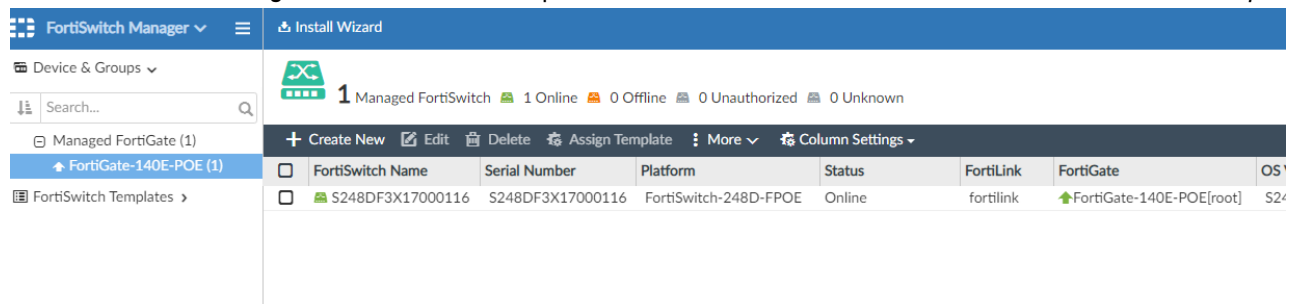
- b. In the banner, click *More > View Health Monitor*, to view the Health monitor.



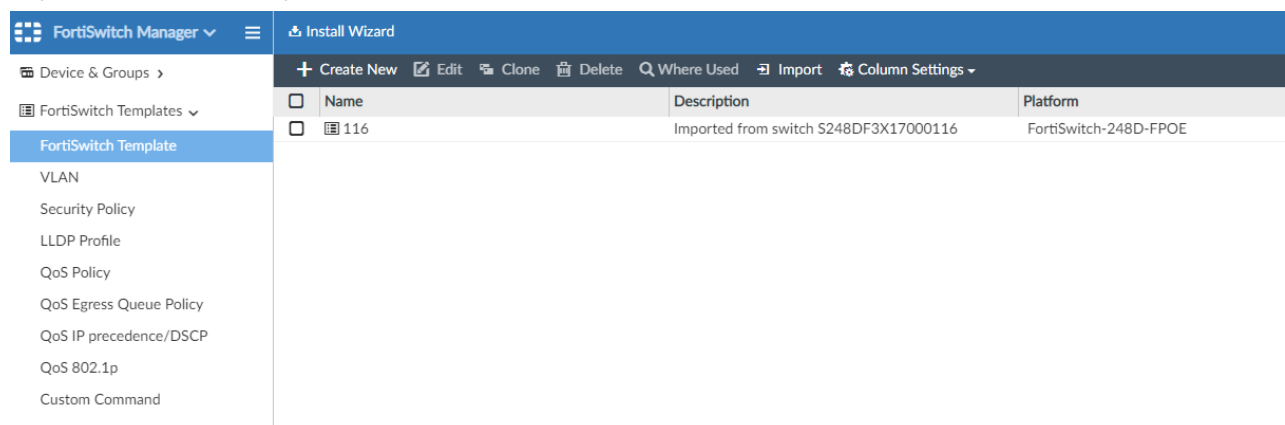
FortiSwitch Manager

To view the GUI changes in FortiSwitch Manager:

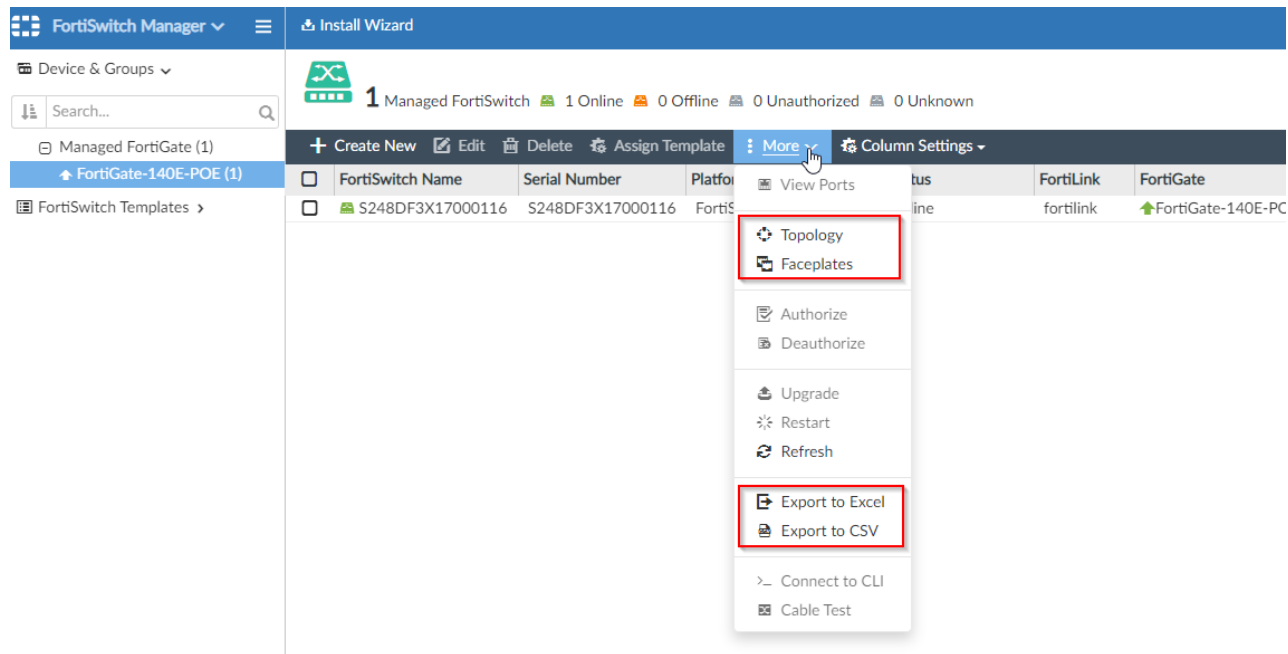
- Go to *FortiSwitch Manager*. The FortiSwitch templates tab is now located in the tree menu under *Devices & Groups*.



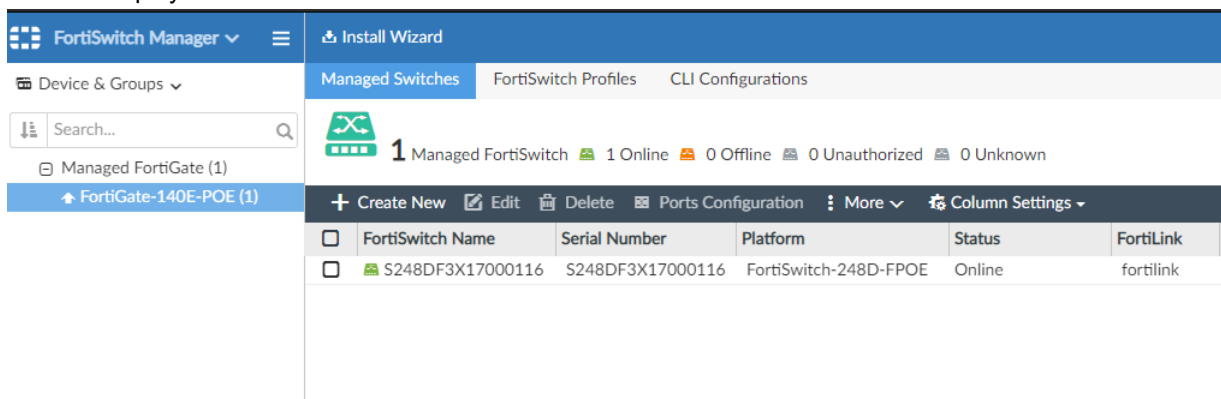
Expand FortiSwitch Templates.



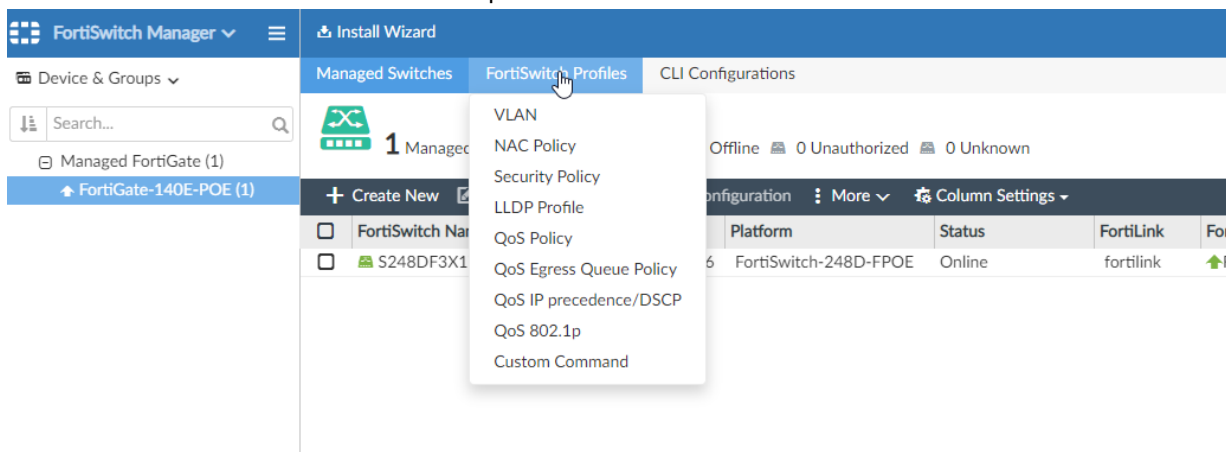
2. In the toolbar, click *More* to access *Topology* and *Faceplates*.
The *Export to Excel* and *Export to CSV* were also added to the list.



3. View FortiSwitch profiles in Per-Device Management mode.
 - a. In the tree menu, click a managed device. The *Managed Switches*, *FortiSwitch Profiles* and *CLI Configurations* tabs are displayed



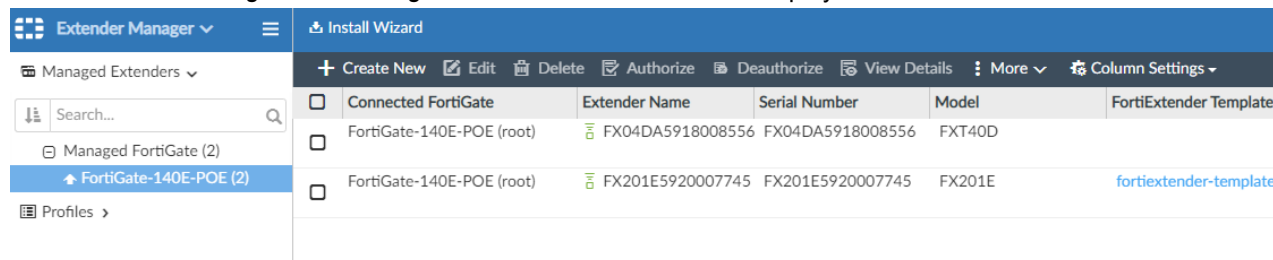
- b. Click the *FortiSwitch Profiles* tab to select a profile.



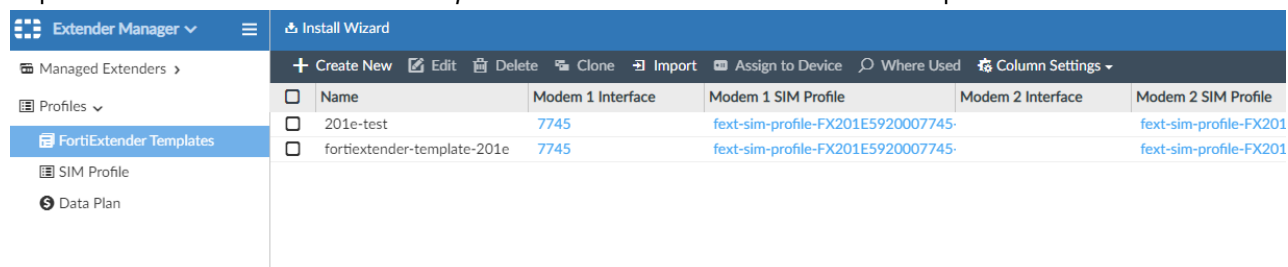
Extender Manager

To view the GUI changes in the Extender Manager:

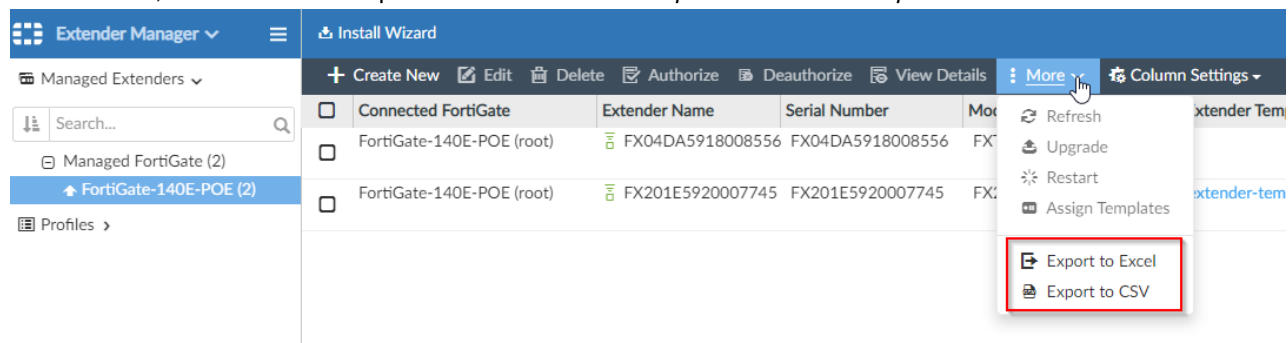
1. Go to *Extender Manager*. The *Managed Extenders* and *Profiles* are displayed in the tree menu.



2. Expand *Profiles*. The *FortiExtender Templates* were added to the list of extender templates.



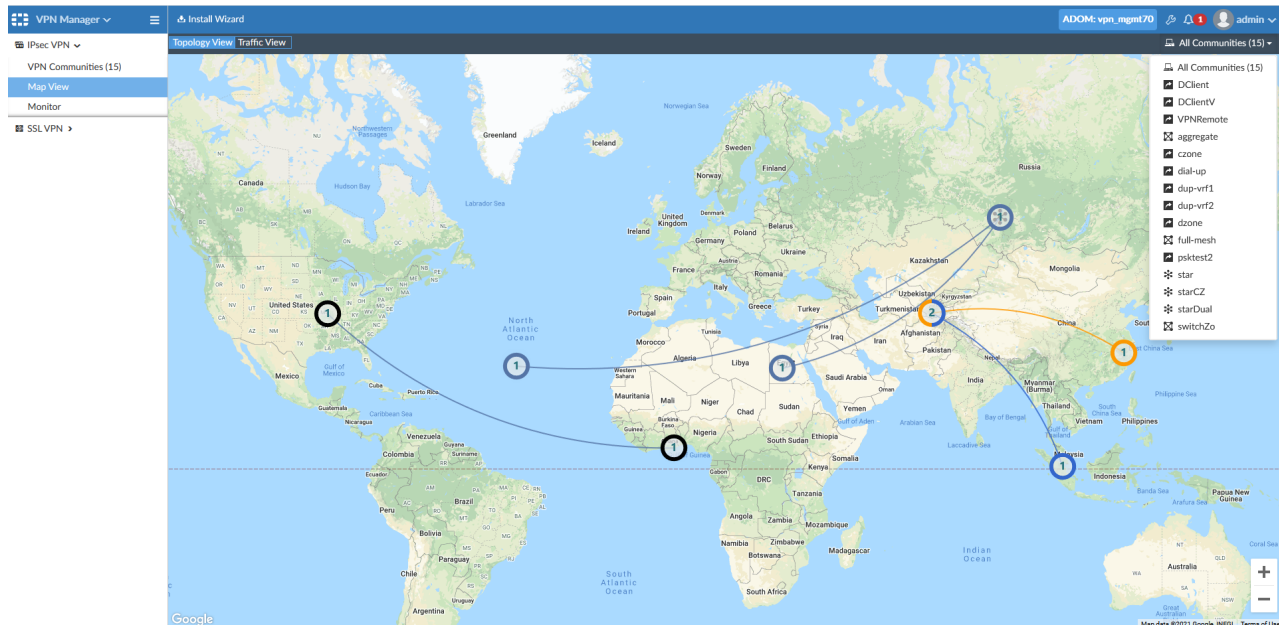
3. In the toolbar, click *More*. The dropdown list now includes *Export to Excel* and *Export to CSV*.



VPN Manager

To view the GUI changes in the VPN Manager:

1. Go to *VPN manager*. The *Monitor*, *Map View*, and *SSO VPN* tabs are now located in the tree menu.
2. Click *Map View* > *All Communities* and select a VPN community. The dropdown is set to *All* by default.



3. Click *Monitor* > *All Communities* and select a VPN community. The dropdown is set to *All* by default.

Status	Device	PI Name	Type	Remote Gateway	Uptime
Down	FGVM08H220311090[root]	ToHQ1	automatic	10.8.2.12	
Up	vlan171_0091[root]	switchZo_2	automatic	100.71.92.1	13d 18h 49m 18s
Up	vlan171_0092[root]	switchZo_1	automatic	100.71.91.1	13d 18h 49m 17s
Down	vlan171_0093[SIMPLY-ENERGY]	longvdompn	automatic	1.2.3.4	
Up	vlan171_0093[vt_1]	starCZ_15	automatic	101.71.94.1	13d 18h 40m 49s
Up	vlan171_0093[vt_1]	starCZ_16	automatic	101.71.95.1	13d 18h 40m 49s
Up	vlan171_0094[vt_1]	starCZ_14	automatic	101.71.93.1	13d 18h 40m 49s
Up	vlan171_0095[PG-traffic]	starCZ_14	automatic	101.71.93.1	13d 18h 40m 49s
Down	vlan171_0096[root]	DCClientV_0_0	dialup	100.71.98.1	13d 18h 23m 07s
Up	vlan171_0096[root]	DCClient_0_0	dialup	100.71.97.1	13d 18h 28m 58s
Up	vlan171_0097[root]	DCClient_0	automatic	100.71.96.1	13d 18h 28m 58s
Down	vlan171_0098[root]	DCClientV_0	automatic	100.71.96.1	13d 18h 23m 07s
Down	vlan171_0099[root]	test1	automatic	10.8.71.102	

FortiManager VM supports Amazon EC2 IMDS version 2

Support for Amazon EC2 Instance Metadata Service (IMDS) version 2 was added to FortiManager virtual machines (VMs) for enhanced security.

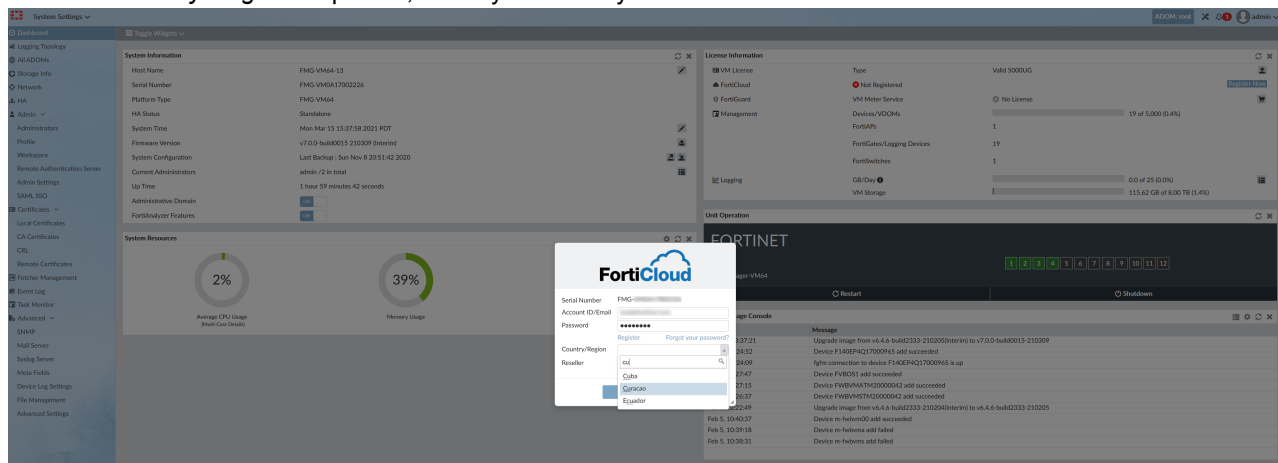
IMDS version 2 uses session-oriented requests. With session-oriented requests, you create a session token that defines the session duration, which can be a minimum of one second and a maximum of six hours. During the specified duration, you can use the same session token for subsequent requests.

Country list for direct registration - 7.0.1

FortiManager now retrieves a list of countries and regions from FortiCare as part of the registration process.

To register a product with FortiCloud:

1. Go to *System Settings*.
2. In the *License Information* widget, click *Register Now*. The registration window opens.
3. From the *Country/Region* dropdown, select your country and click *OK*.



Event log easier to read - 7.0.1

The FortiManager event log includes the following new columns to make messages easier to read:

- *Operation*
- *Performed On*
- *Changes*

Go to *System Settings > Event log* to view the new columns:

#	Date Time	Level	User	Sub Type	Description	Operation	Performed On	Changes
1	2021-04-29 10:22:29	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update package from fds(000000000000-2104291723): 01000000ALCI000000(AlCI Object), version:000000000000-2104291723
2	2021-04-29 10:13:43	information	admin-GUI(10.2.0.250)	system	User login/logout successful	login	GUI(10.2.0.250)	'admin' login accepted from GUI(10.2.0.250)
3	2021-04-29 10:13:42	information	fgdlinkd	fgd	Package update response from FortiGuard server received	Update Response	FDS Server	Receive an update package from FDS: (CURL)000000FortiGuard(CURL),version:00001.00060-2001131740
4	2021-04-29 10:12:17	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update package from fds(000000000000-2104291713): 01000000ALCI000000(AlCI Object), version:000000000000-2104291713
5	2021-04-29 10:05:23	notice	System	dvm	Device Manager dvm log at notice level	Modify device	FGVM4VTM20...	Edited device settings (SN FGVM4VTM20003032)
6	2021-04-29 10:05:12	notice	System	dvm	Device Manager dvm log at notice level	Modify device	FGVM4VTM20...	Edited device settings (SN FGVM4VTM20003032)
7	2021-04-29 10:01:55	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update package from fds(00018.00070-2104290050): 06004000APDB00100(Application Meta), version:00018.00070-2104290050
8	2021-04-29 10:01:55	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update package from fds(00018.00070-2104290054): 06000000NIDS025000(IPS Extended Meta), version:00018.00070-2104290054
9	2021-04-29 10:01:55	information	update_manager	fgd	Package update response from FortiGuard server received	Update Response	12.34.97.16	Receive an update package from fds(00018.00070-2104290054): 06000000NIDS024000(IPS Regular Meta), version:00018.00070-2104290054

Local FortiGuard Distribution Server enhancements - 7.0.1

The *FortiGuard* module includes several enhancements when FortiManager is used as a dedicated FortiGuard Distribution Server (FDS):

- Support to download packages from FortiGuard for FortiDeceptor and FortiTester - see [FortiDeceptor and FortiTester on page 147](#).
- Support to prioritize downloads from FortiGuard - see [Download prioritization on page 148](#).
- Support to download IoT packages - See [IoT packages on page 150](#).

FortiDeceptor and FortiTester

You can now use FortiManager as a local FDS server for FortiDeceptor and FortiTester. Go to *FortiGuard > Settings* to view the *FortiDeceptor* and *FortiTester* options:

FortiGuard <ul style="list-style-type: none"> Licensing Status Package Management > Query Server Management > Firmware Images Download Prioritization Settings 	<div> <div>ADOM: root</div> <div>1</div> <div>2</div> <div>admin</div> </div> <h3>FortiGuard Server and Service Settings</h3> <div> <div>Enable Communication with FortiGuard Server</div> <div> <input checked="" type="checkbox"/> ON </div> </div> <div> <div>Communication with FortiGuard Server</div> <div> <input type="radio"/> Global Servers <input checked="" type="radio"/> Servers Located in US Only </div> </div> <div> <div>Enable AntiVirus and IPS Service</div> <div> <input checked="" type="checkbox"/> ON </div> </div> <div> <div>FortiGate</div> <div> <input type="checkbox"/> 5.4 <input type="checkbox"/> 5.6 <input type="checkbox"/> 6.0 <input type="checkbox"/> 6.2 <input checked="" type="checkbox"/> 6.4 <input checked="" type="checkbox"/> 7.0 </div> </div> <div> <div>FortiMail</div> <div> <input type="checkbox"/> All v4 <input type="checkbox"/> All v5 <input type="checkbox"/> 6.0 <input type="checkbox"/> 6.2 <input checked="" type="checkbox"/> 6.4 </div> </div> <div> <div>FortiSandbox</div> <div> <input type="checkbox"/> All v1 <input type="checkbox"/> All v2 <input checked="" type="checkbox"/> 3.0 <input checked="" type="checkbox"/> 3.1 <input checked="" type="checkbox"/> 3.2 <input checked="" type="checkbox"/> All v4 </div> </div> <div> <div>FortiClient</div> <div> <input type="checkbox"/> All v4 <input type="checkbox"/> 5.0 <input type="checkbox"/> 5.2 <input type="checkbox"/> 5.4 <input type="checkbox"/> 5.6 <input type="checkbox"/> 6.0 </div> </div> <div> <div>FortiDeceptor</div> <div> <input checked="" type="checkbox"/> All v3 </div> </div> <div> <div>FortiTester</div> <div> <input checked="" type="checkbox"/> All v4 </div> </div> <div> <div>Enable Web Filter Service</div> <div> <input checked="" type="checkbox"/> ON </div> </div> <div> <div>Web Filter Database</div> <table> <tr> <td>Version</td> <td>24.61893</td> </tr> <tr> <td>Last Updated</td> <td>2021-08-04 15:55:09</td> </tr> </table> <div>Apply</div> </div>	Version	24.61893	Last Updated	2021-08-04 15:55:09
Version	24.61893				
Last Updated	2021-08-04 15:55:09				

You can also configure downloads for FortiDeceptor and FortiTester by using the CLI:

```
config fmupdate fds-setting
  set system-support-fdc 3.x <---- new
  set system-support-fgt 6.4 7.0
  set system-support-fml 6.4
  set system-support-fsa 4.x 3.0 3.1 3.2 <---- version 4.0 is new
  set system-support-fts 4.x <---- new
end
```

Download prioritization

When FortiManager is acting as a local FDS, you can prioritize downloads from FortiGuard to FortiManager by product and version and/or package. This is useful when you have limited network access.

Before you can specify a priority list, you must enable products and versions for prioritization.

To enable products and versions for prioritization:

1. Go to *FortiGuard > Settings*.
2. Under *Enable AntiVirus and IPS Service*, select the versions for each product, and click *Apply*.

To enable product download prioritization:

1. Go to *FortiGuard > Download Prioritization*, and toggle *Enable by Product* to *ON*.

2. Add products to the priority list:
 - a. In the toolbar, click *Create New*.
The *Create Download Prioritization* dialog box is displayed.

- b. Beside *Products*, click the box, and select one or more products and versions, and click *OK*.
The selected products are displayed in the product list.

- c. Click **OK**.

The products are displayed in the priority list.

Enable By Product ON		
+ Create New Delete Move To Column Settings		
<input type="checkbox"/> #	Product	Version
<input type="checkbox"/> 1	FortiClient	5.2
<input type="checkbox"/> 2	FortiGate	6.0
<input type="checkbox"/> 3	FortiMail	5.1
<input type="checkbox"/> 4	FortiDeceptor	3.1
<input type="checkbox"/> 5	FortiMail	5.3
<input type="checkbox"/> 6	FortiManager	6.2

3. Specify the download priority for products:

- a. Select one or more products, and click **Move To**.

The **Move To** dialog box is displayed.

Move To

From #

4,5

To #

Before

After

OK

Cancel

- b. Beside **To #**, select **Before** or **After**, and click the box to use the up and down arrows to position the selected products in the priority list.

- c. Click **OK**.

The products are moved, and the updated priority list is displayed.

You can remove products from the priority list. Select one or more products, and click **Delete**.

4. (Optional) Add packages to the priority list.

To enable package download prioritization:

1. Go to **FortiGuard > Download Prioritization**, and toggle **Enable by Package** to **ON**.

2. Add packages to the priority list:

- a. In the toolbar, click **Create New**.

The **Create Download Prioritization** dialog box is displayed.

Create Download Prioritization

Packages

Click here to select

OK

Cancel

- b. Beside **Packages**, click the box, and select one or more packages, and click **OK**.
The selected packages are displayed in the packages list.

- c. Click **OK**.

The packages are displayed in the priority list.

Enable By Package ON							
+ Create New Delete Move To Column Settings							
#	Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size
<input type="checkbox"/> 1	AntiVirus Signature Dat	FortiClient	6.0.0+	EMS	06000000FVDB00000	NA	NA
<input type="checkbox"/> 2	00000000FCNI00000	FortiGate			00000000FCNI00000	NA	NA
<input type="checkbox"/> 3	Internet Service DB	FortiManager	6.0.0+	Internet Service DB	06000000FFDB00305	7.01711 (2021-07-14 13:31:00)	6.91 KB

3. Specify the download priority for the packages:

- Select one or more packages, and click *Move To*.

The *Move To* dialog box is displayed.

Move To

From #

2

To #

Before

After

OK

Cancel

- Beside *To #*, select *Before* or *After*, and click the box to use the up and down arrows to position the selected packages in the priority list.
- Click *OK*.

The packages are moved, and the updated priority list is displayed.

You can remove packages from the priority list. Select one or more packages, and click *Delete*.

4. (Optional) Add products and versions to the priority list.

IoT packages

The *FortiGuard* module now supports the download of packages for the Internet of Things (IoT) service. Following is a summary of how FortiManager handles the IoT packages:

- FortiManager downloads packages from FortiGuard.
- FortiManager merges the downloaded packages into *Run Database*.
- FortiManager provides the query service.



Downloads of IoT packages from FortiGuard to FortiManager are currently supported only when Anycast is enabled on FortiManager.

The following new options have been added to the `diagnose` command:

```
diagnose fmupdate fgd-dbver [wf|as1|as2|as4|av-query|fq|av2|geoip|iots|iotr|iotm]
diagnose fmupdate fgd-del-db [wf|as|av-query|file-query|av2|iot]
```

Use the `diagnose fmupdate fgd-dbver` command to view the following databases for IoT packages:

- iots:** IoT single MAC database
object ID: 00000000IOTS0000

Contains IoT info with entry of a single MAC. Considered a *delta* object because each version contains parts of data, and FortiManager merges all valid data, which is the same as the URL query service.

- iotr:** IoT range MAC database
object ID: 00000000IOTR0000

Contains IoT info with entry of a MAC range. Considered a *regular* object, and FortiManager uses only the latest version.

- **iotm: IoT mapping database**
object ID: 00000000IOTR0000

Regular object used to map the info data to strings in tag-length-value (TLV) format.

To configure IoT package download:

1. Enable Anycast on FortiManager:

```
config fmupdate fds-setting
    set fortiguard-anycast enable
end
```

2. Enable download of IoT packages:

```
config fmupdate service
    set query-iot enable
end
```

3. Configure downloading of IoT packages:

```
config fmupdate web-spam fgd-setting
    set iot-log nofilequery
    set iot-preload enable
    set restrict-iots-dbver <string>
end
```

NSX-T service template with VDOM support - 7.0.1

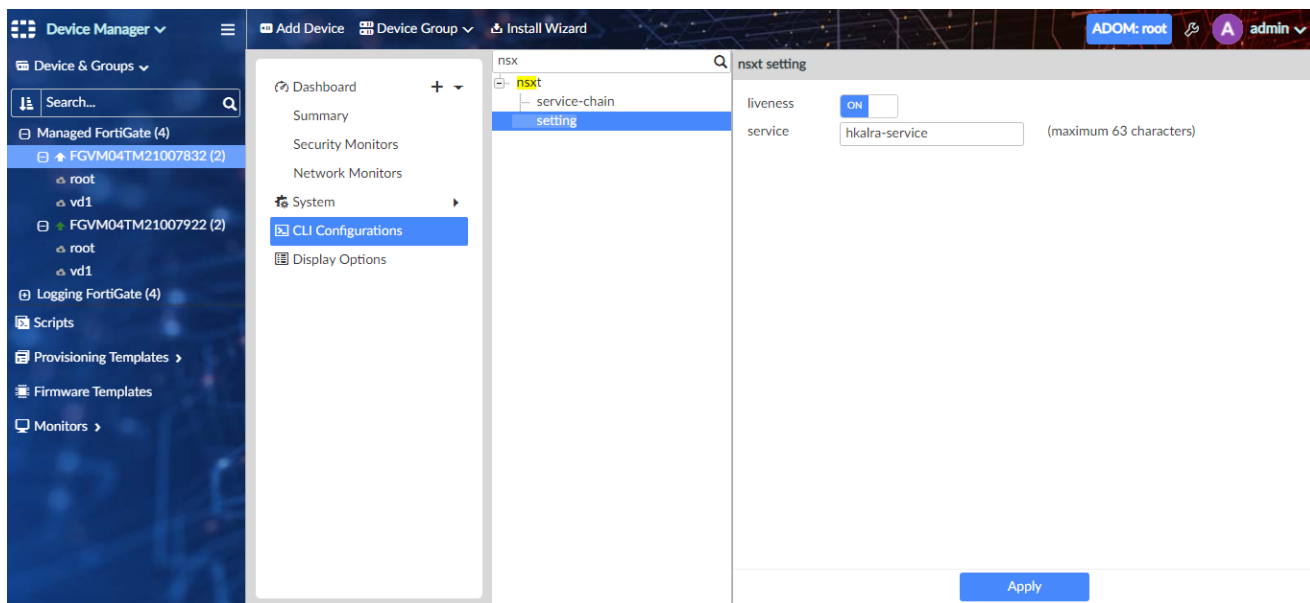
FortiManager 7.0.1 includes an NSX-T Service Template with VDOM support.

This section includes the following topics:

- [Liveness detection on page 151](#)
- [Service chain on FortiGate VMs on page 152](#)
- [Manage devices using an NSX-T service template on page 153](#)
- [CLI configuration on page 156](#)

Liveness detection

Liveness detection can be enabled and disabled for each VM. The configuration can be managed in *Device Manager* by selecting a FortiGate and going to *CLI Configuration > nsxt > setting*.

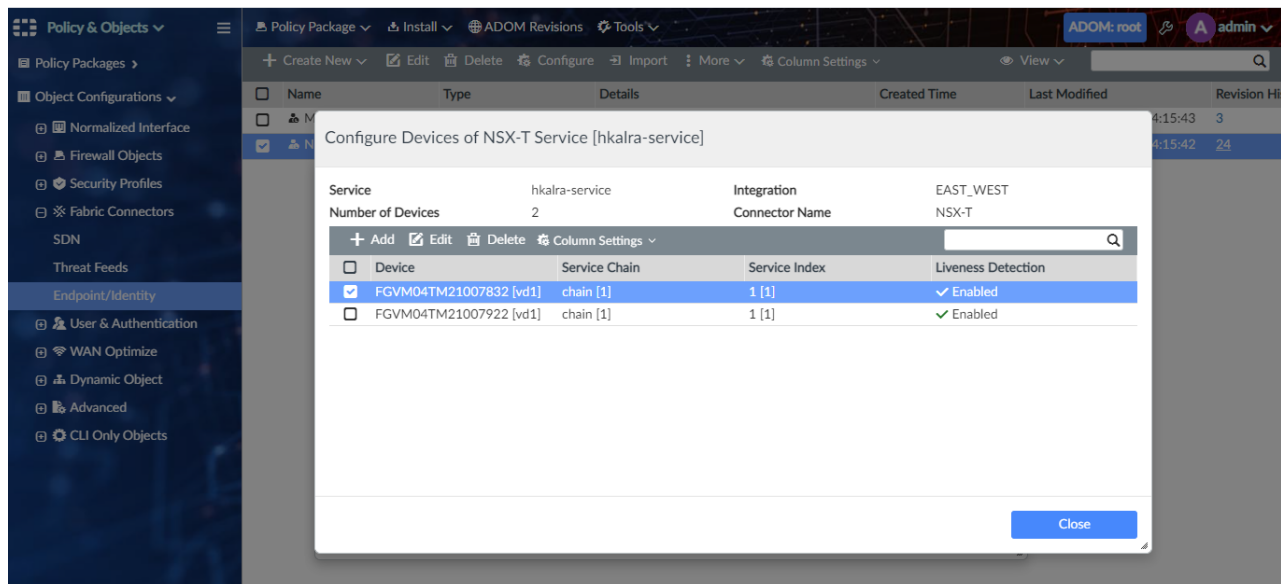


Service chain on FortiGate VMs

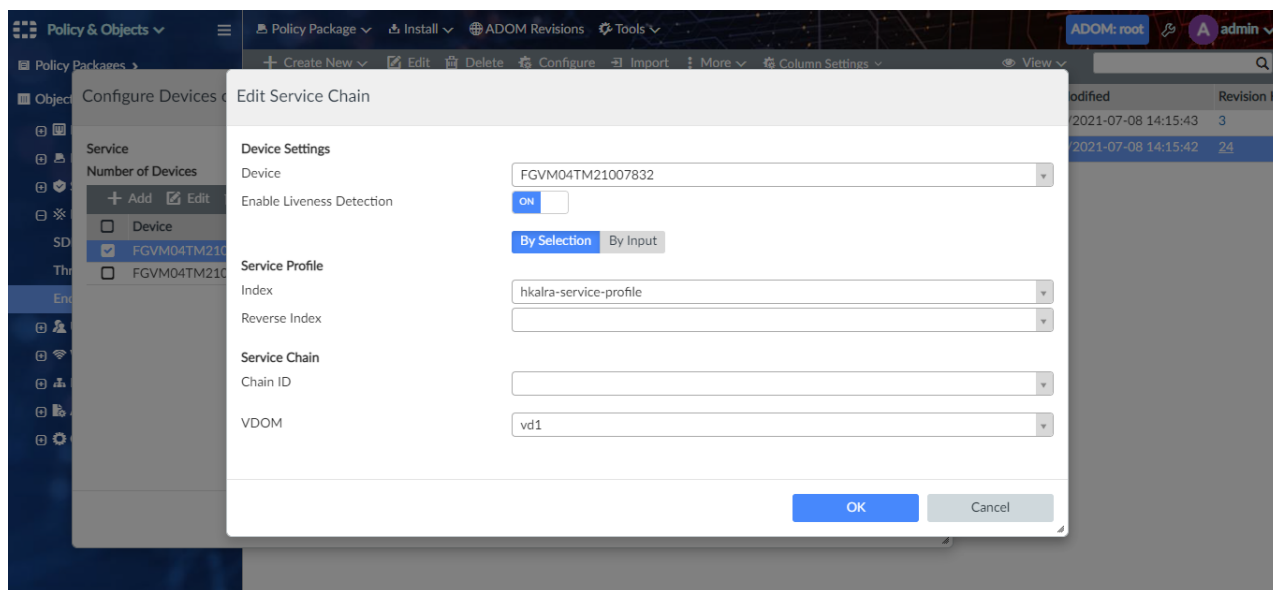
Service chain configuration on FortiGate VMs launched through NSX-T can be managed under the service.

To edit service chains for FortiGate VMs:

1. Go to *Policy & Objects > Object Configurations > Fabric Connectors > Endpoint/Identity*.
2. Select and edit the NSX-T connector, and then select and configure the service.



3. Select and edit a device.

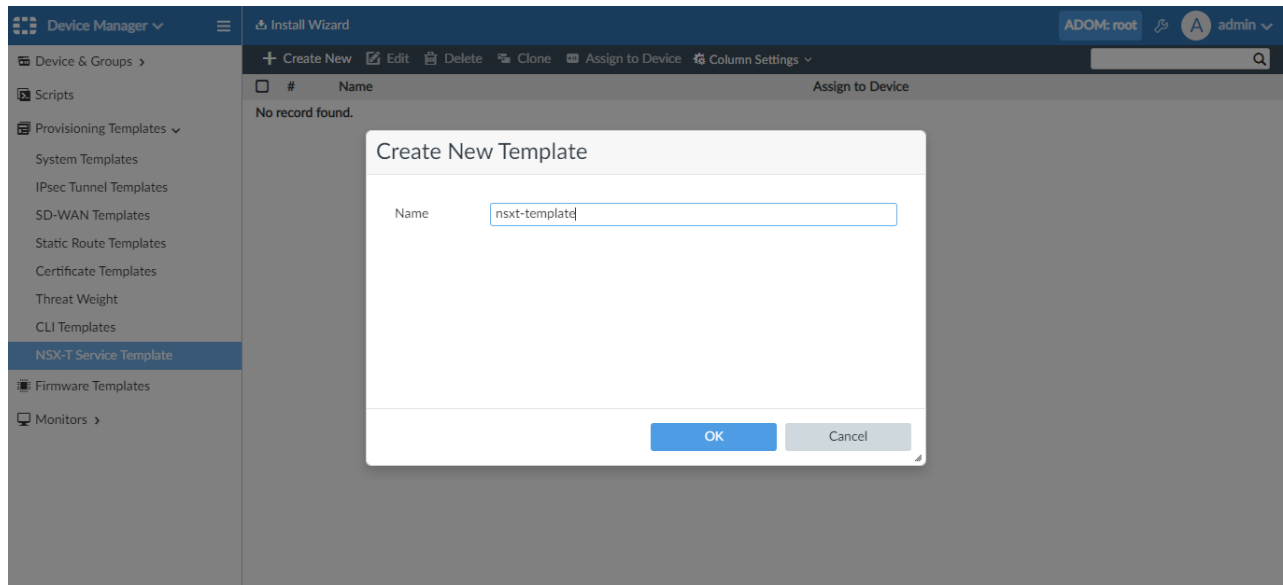


Manage devices using an NSX-T service template

NSX-T templates can be created, cloned, deleted, and assigned in *Device Manager > Provisioning Templates > NSX-T Service Template*.

To create a new NSX-T service template:

1. Go to *Device Manager > Provisioning Templates > NSX-T Service Template*.
2. Click *Create New* in the toolbar.
3. In the *Create New Template* pane, type a name for the template.
4. Click *OK* to create the new NSX-T service template.

**To edit an NSX-T service template:**

1. Go to *Device Manager > Provisioning Templates > NSX-T Service Template*.
2. Select an NSX-T service template and click *Edit*.
The *Edit NSX-T Service Template* pane opens.

- Adjust the settings as required, and click **OK** to save your changes.

Edit NSX-T Service Template

NSXT Connector
None

Firmware
None

Description
0/255

VDOMs

+ Create New
Edit
Delete

<input type="checkbox"/>	VDOM	Virtual Wire Pair	Policy Package
<input type="checkbox"/>	root	nsxt	

Service Chain

+ Create New
Edit
Delete

<input type="checkbox"/>	Name	Use SDWAN
No record found.		

OK

Cancel

To create a new VDOM in an NSX-T service template:

- Click **Create New** under the **VDOMs** section. The **Create New VDOM** pane opens.
- Fill in the VDOM name and select the policy package from the dropdown which will be applied to the template.
- The Virtual Wire Pair will be automatically filled based on the VDOM name.

Create New VDOM

VDOM Name

demo-vdom

Policy Package

FortiGate-VM64

Virtual Wire Pair

demo-vdom_vwp

Interfaces

Edit

<input type="checkbox"/>	Name	Remote IP	Interface	Dynamic Interface
<input type="checkbox"/>	demo-vdom_int	10.0.0.1	port2	
<input type="checkbox"/>	demo-vdom_ext	10.0.0.1	port2	

OK

Cancel



Dynamic interface mapping is mandatory to create the VDOM. Select the interface name and click **Edit** to configure the dynamic interface mapping for internal and external interfaces.



The Dynamic Interface dropdown will only show normalized interfaces which have default mappings and where the default mapping name is the same as the name of the interface on the *Edit Interface* page. You can create a new interface using the add icon in the dropdown.

To assign an NSX-T service template to a device:

1. Go to *Device Manager > Provisioning Template > NSX-T Service Template*.
2. Select a template to assign to managed devices.
3. Right-click anywhere in the template list window and select *Assign to Device* from the menu, or click *Assign to Device* from the toolbar above.
The *Assign to Device* dialog appears.
4. Select the managed devices to which you want to assign the selected template from the *Available Entries* field, and move those entries to the *Selected Entries* field.



For a device to show up in the list it should meet the following conditions as also mentioned on the *Edit Installation Target* panel.

- VDOM feature should be enabled on the FortiGate.
- The FortiGate should match the platform type with the one mentioned in the template.
- The NSX-T service name should match with devices.

CLI configuration

Service Configured on Fortigate:

```
config nsxt setting
  set liveness enable
  set service "hkalra-service"
end
```

Configuration pushed to Fortigate:

```
FGVM04TM21007922 $ config vdom
FGVM04TM21007922 (vdom) $ edit vd1
current vf=vd1:3
FGVM04TM21007922 (vd1) $ end
FGVM04TM21007922 $ config global
FGVM04TM21007922 (global) $ config system interface
FGVM04TM21007922 (interface) $ edit "ssl.vd1"
FGVM04TM21007922 (ssl.vd1) $ set vdom "vd1"
FGVM04TM21007922 (ssl.vd1) $ set type tunnel
FGVM04TM21007922 (ssl.vd1) $ set alias "SSL VPN interface"
FGVM04TM21007922 (ssl.vd1) $ set snmp-index 110
FGVM04TM21007922 (ssl.vd1) $ next
FGVM04TM21007922 (interface) $ edit "vd1_int"
FGVM04TM21007922 (vd1_int) $ set vdom "vd1"
FGVM04TM21007922 (vd1_int) $ set type geneve
FGVM04TM21007922 (vd1_int) $ set snmp-index 111
FGVM04TM21007922 (vd1_int) $ set interface "port2"
FGVM04TM21007922 (vd1_int) $ next
FGVM04TM21007922 (interface) $ edit "vd1_ext"
```



```
FGVM04TM21007922 (vd1_ext) $ set vdom "vd1"
FGVM04TM21007922 (vd1_ext) $ set type geneve
FGVM04TM21007922 (vd1_ext) $ set snmp-index 112
FGVM04TM21007922 (vd1_ext) $ set interface "port2"
FGVM04TM21007922 (vd1_ext) $ next
FGVM04TM21007922 (interface) $ end
FGVM04TM21007922 (global) $ config nsxt service-chain
FGVM04TM21007922 (service-chain) $ edit 1
FGVM04TM21007922 (1) $ config service-index
FGVM04TM21007922 (service-index) $ edit 1
FGVM04TM21007922 (1) $ set reverse-index 2
FGVM04TM21007922 (1) $ set name "1"
FGVM04TM21007922 (1) $ set vd "vd1"
FGVM04TM21007922 (1) $ next
FGVM04TM21007922 (service-index) $ end
FGVM04TM21007922 (1) $ next
FGVM04TM21007922 (service-chain) $ end
FGVM04TM21007922 (global) $ end
```



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.